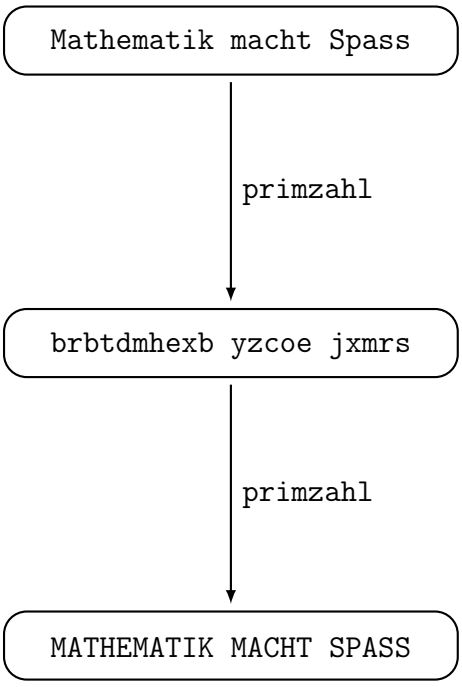
Universität Stuttgart

Schülerzirkel MATHEMATIK

Zahlentheorie und Kryptographie

Peter Lesky



Vorwort

Der vorliegende Text beschreibt einen Kurs über Kryptographie, der bereits mehrere Male im Schülersminar Mathematik für die Klassenstufen 8–10 abgehalten wurde. Der Kurs umfasst 7 dicht gepackte Doppelstunden. Das Ziel des Kurses ist es, zu verstehen, wie und warum der Diffie-Hellman-Merkle Schlüsselaustausch, das Elgamal- und das RSA-Verfahren funktionieren. Das Skript ist dazu gedacht, eine Anleitung zum Unterricht zu geben bzw. die Vorbereitung des Unterrichts zu erleichtern.

Das Schülerseminar wurde jedes Mal von einer Gruppe aus Studierenden abgehalten. In jedem Durchgang wurden Verbesserungen und neue Ideen eingearbeitet. Sehr wertvoll war das Feedback aus der Gruppe der Studierenden, nachdem eine(r) von Ihnen die Einheit abgehalten hatte. Daraus resultierten methodische und didaktische Überlegungen, die ins Skript übernommen wurden. Im letzten Durchgang wurden sogenannte *schriftliche Aufgaben* ergänzt, die für eine online-Version des Kurses gedacht sind. Der online-Kurs ist auf der Homepage des Schülerzirkels Mathematik zu finden.

Als Grundlage wurden die Bücher

- Einführung in die Kryptographie, Johannes Buchmann, Springer, 2004
- Zahlentheorie für Einsteiger, Andreas Bartholomé ; Josef Rung ; Hans Kern, Vieweg, 2001

verwendet. Das Buch von Buchmann ist für jüngere Schüler etwas zu trocken, man findet aber alles Nötige darin. Das andere Buch ist leichter zu lesen, dafür ist nicht der ganze Stoff unseres Seminars enthalten.

Bei meinen Vorbereitungen war mir wichtig, dass den Schülerinnen und Schülern Mathematik im eigentlichen Sinn nahegebracht wird: Viele konkrete Probleme können durch Ausprobieren gelöst werden. Aber danach müssen die Begriffe und die Problemstellung richtig definiert, die Lösungsmethoden in möglichst großer Allgemeinheit formuliert und ihre Gültigkeit bewiesen werden. Erst dann ist das Problem als gelöst anzusehen:

$$\text{Probieren} \to \text{Vermuten} \to \text{Definieren} \to \text{Satz formulieren} \to \text{Beweisen}$$

Ich danke allen Studierenden, die dieses Thema in unserem Schülerseminar unterrichtet haben. Sie haben wesentlich zur Weiterentwicklung des Inhalts beigetragen. Außerdem danke ich meinem Kollegen Matthias Künzer für wertvolle Hinweise zur Verbesserung des Skriptes.

Ich wünsche allen, die dieses Skript lesen oder für den Unterricht verwenden, gutes Verstehen und viel Freude an der Mathematik.

August 2024 Peter Lesky

Erste Durchführung im Schülerseminar **2006**,
Erste schriftliche Fassung **2013**, Neubearbeitung **2019**,
Überarbeitung und schriftliche Aufgaben **2024**.

Schülerzirkel Mathematik: `www.f08.uni-stuttgart.de/schulen/schuelerzirkel-mathematik/`

Inhaltsverzeichnis

1 Allgemeine Vorbemerkungen und Notationen

Die Lösungen aller Aufgaben außer den schriftlichen sind im Skriptteil (Kapitel 2 bis Kapitel 8) enthalten. Sind im Aufgabentext Freiräume zum Eintragen der Lösung vorgesehen, so sind die Lösungen direkt in blauer Farbe eingetragen. Andernfalls stehen die Lösungen nach der Aufgabe.

In den Ausarbeitungen der Einheiten (Kapitel 11 bis Kapitel 17) sind alle Aufgaben ohne Lösungen in den Arbeitsblättern zu den Einheiten enthalten. Hier befinden sich auch Zeitpläne für den Stundenverlauf und die Planung des Tafelaufschriebs. Die Zeitpläne sind im Schülerseminar getestet. Im Normalfall muss man mehr Zeit einplanen.

Bei allen Gleichungen in diesem Kurs werden ganzzahlige Lösungen gesucht. Schüler:innen, die bereits Geradengleichungen kennen, tendieren dazu, die Gleichungen nach y aufzulösen und nehmen dabei das Auftreten von Brüchen in Kauf. Zur Vorbeugung wird in allen Aufgaben betont, dass ganzzahlige Lösungen gesucht sind.

Im Präsenz-Unterricht wurden die Aufgaben von den Schülern in Dreier- oder Zweiergruppen gelöst. Manchmal wurden verschiedene Aufgabenteile von verschiedenen Gruppen bearbeitet, und im Anschluss präsentierte dann aus jeder Gruppe eine Schülerin oder ein Schüler die Lösung an der Tafel oder gab das Ergebnis an.

In Baden-Württemberg wird in den Schulbüchern die Null zu den natürlichen Zahlen gezählt. Wir verwenden die Bezeichnung $\mathbb{N}_+$ für die positiven natürlichen Zahlen. In der Schule wird stattdessen $\mathbb{N}^*$ verwendet, entsprechend $\mathbb{Z}^*$ für die ganzen Zahlen ohne die Null.

Für die Äquivalenzklassen bezüglich der Kongruenzrelation modulo m wurde die Schreibweise $[a]$ mit $a \in \mathbb{Z}$ gewählt. Auf einen Index m oder etwas ähnliches wurde verzichtet, um die Notation nicht zu überladen. Diese Notation hat allerdings den Nachteil, dass man im Zweifelsfall immmer dazuschreiben muss, bezüglich welchem Modul die Äquivalenzklasse zu bilden ist.

2 Unterrichtseinheit 1: Der euklidische Algorithmus

2.1 Vorbemerkungen

Der gesamte Kurs baut auf der Lösungstheorie für lineare diophantische Gleichungen auf. Dies ist zum einen ein interessanter Einstieg für die Schüler:innen, zum anderen bilden die hier gewonnenen Erkenntnisse eine ausreichende Grundlage, um die im weiteren Verlauf des Kurses benötigten Sätze zu beweisen.

Die Lösungstheorie für lineare diophantische Gleichungen wird in zwei Doppelstunden entwickelt. In der ersten wird der euklidische Algorithmus zur Bestimmung des größten gemeinsamen Teilers eingeführt, während in der zweiten Doppelstunde der erweiterte euklidische Algorithmus zu Berechnung von Lösungen verwendet wird.

Der erweiterte euklidische Algorithmus wird nur mit positiven Zahlen durchgeführt. Für die Berechnung der Lösungen diophantischer Gleichungen $ax + by = c$ ist dies keine Einschränkung. Man kann im allgemeinen Fall eine oder beide der Variablen mit -1 multiplizieren, um eine diophantische Gleichung mit positiven Koeffizienten und positiver rechter Seite zu erhalten.

2.2 Lineare diophantische Gleichungen

Mündlich: Wir stellen zunächst mathematische Grundlagen zur Verfügung, die wir erst später anwenden. Im Schülerseminar ist der Unterricht etwas näher an Universitätsunterricht. Es gibt mehr zum Mitschreiben und bei manchen Dingen sieht man erst später, wozu sie benötigt werden.

> **Anmerkung**
> Der Einfachheit halber sprechen wir von *diophantischen Gleichungen* und lassen *linear* weg.

Tafelanschrieb

Zahlentheorie und Kryptographie

1. Diophantische Gleichungen

Gegeben:	$a, b, c \in \mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$
Gesucht:	$x, y \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
so dass	$ax + by = c$
Vereinbarung:	Schreibe die Lösungen als Zahlenpaare $(x \mid y)$

> **Anmerkung**
> Eventuell sollte die aufzählende Mengenschreibweise erklärt werden, falls noch nicht alle Schüler:innen damit vertraut sind.

Mündlich: In der folgenden Aufgabe könnt ihr ausprobieren, ob ihr Lösungen von diophantischen Gleichungen finden könnt.

Aufgabe 1.1 (*Arbeitsblatt 1.1 (Diophantische Gleichungen), Aufgabe 1*)

Versuche, jeweils ganzzahlige Lösungen $(x \mid y)$ der angegebenen Gleichung zu finden.
Falls du vermutest, dass es keine Lösung gibt, begründe deine Vermutung.

a) $x + 3y = 10$: $x = 10 - 3y$, z.B. $(x \mid y) = (7 \mid 1), (4 \mid 2), (1 \mid 3), (13 \mid -1)$

b) $3x + 7y = 1$: z.B. $(x \mid y) = (-2 \mid 1), (5 \mid -2), (12 \mid -5), (-9 \mid 4)$

c) $18x + 12y = 3$: Keine Lösung: Linke Seite gerade, rechte ungerade

Zusatzaufgaben:

d) $5x + 5y = 1$: Keine Lösung: Linke Seite ist durch 5 teilbar, rechte nicht

e) $5x + 15y = 50$: Teile die Gleichung auf beiden Seiten durch 5: $x + 3y = 10$
$\Rightarrow$ Gleichung ist die selbe wie in a), also die selben Lösungen

f) $18x + 12y = 66$: Teile Gleichung durch 6: $3x + 2y = 11$,
z.B. $(x \mid y) = (-1 \mid 7), (1 \mid 4), (3 \mid 1), (5 \mid -2)$

Datei: `Kryptographie10-DiophantischeGleichung`

Lösung: Ist bereits im Aufgabentext enthalten.

Mündlich: Wir sehen: Es gibt nur Lösungen, wenn jeder Teiler von a und b auch Teiler von c ist.

Wir wollen dies in mathematischer Sprache aufschreiben und benötigen dazu ein paar Vorbereitungen.

Tafelanschrieb

Definition: 1) Seien $a \in \mathbb{Z}$, $k \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Dann heißt k Teiler von a, geschrieben $k \mid a$, falls es ein $a' \in \mathbb{Z}$ gibt, so dass $a = a' \cdot k$.

Beispiele: $a = 35$ hat die Teiler $1, 5, 7, 35$, denn
$a = 35 \cdot 1 \quad (a' = 35)$
$a = 7 \cdot 5 \quad (a' = 7)$
$a = 5 \cdot 7 \quad (a' = 5)$
$a = 1 \cdot 35 \quad (a' = 1)$

$a = -35$ hat die selben Teiler.

$a = 0$ hat alle positiven natürlichen Zahlen als Teiler: $\underbrace{0}_{a} = \underbrace{0}_{a'} \cdot k$.

Vorgehen: Die Beispiele werden gemeinsam erarbeitet.

Tafelanschrieb

2) Seien $a, b \in \mathbb{Z}$, nicht beide 0. Dann ist der größte gemeinsame Teiler von a, b definiert durch

$$\mathrm{ggT}(a, b) := \max \underbrace{\{k \in \mathbb{N}_+ : k \mid a \text{ und } k \mid b\}}_{\text{Menge der gemeinsamen Teiler von } a \text{ and } b}.$$

Vorgehen: Die Mengenschreibweise sollte verbalisiert werden: *Die Menge aller Elemente k von $\mathbb{N}_+$, für die gilt, dass k Teiler von a und k Teiler von b ist.* Danach kann die Unterklammerung und der Text darunter ergänzt werden.

Mündlich: Warum dürfen a und b nicht beide Null sein? Im Fall $a = b = 0$ ist die Menge der gemeinsamen Teiler ganz $\mathbb{N}_+$ und besitzt kein Maximum.

Tafelanschrieb

Beispiel: $a = 70,\ b = 98$:

a hat die Teiler $1, 2, 5, 7, 10, 14, 35, 70$,
b hat die Teiler $1, 2, 7, 14, 49, 98$,
Menge der gemeinsamen Teiler: $\{1, 2, 7, 14\}$,
Größtes Element der Menge: $\mathrm{ggT}(70, 98) = 14$.

Anmerkung

Jeder gemeinsame Teiler a und b ist Teiler von $\mathrm{ggT}(a, b)$.
Beweis mit Hilfe der Primfaktorzerlegungen von a und b. Die Kenntnis der Primfaktorzerlegung wird als Kenntnis aus der Schule vorausgesetzt.

Anmerkung

In diesem Skript sind Teiler immer positiv. Üblicherweise lässt man auch negative Zahlen als Teiler zu. Aber beim Teilen mit Rest wird man immer nur durch positive Zahlen teilen, auch zur einfachen Formulierung des zugehörigen Satzes (siehe weiter unten). Damit das nicht zur Verwirrung führt, teilen wir immer nur durch positive natürliche Zahlen.

Tafelanschrieb

Satz: Aus $k \mid a$ und $k \mid b$ und $x, y \in \mathbb{Z}$ folgt $k \mid (ax + by)$.

Beweis:
$$\begin{aligned} & k \mid a \ \Rightarrow\ a = a'k \\ & k \mid b \ \Rightarrow\ b = b'k \\ \Rightarrow\ & ax + by \ =\ a'kx + b'ky \ =\ \underbrace{(a'x + b'y)}_{\in\mathbb{Z}}k \\ \Rightarrow\ & k \mid (ax + by) \qquad \square \end{aligned}$$

Mündlich: Nun sind wir genügend gut vorbereitet, dass wir uns um die Lösbarkeit diophantischer Gleichungen zu kümmern können.

Tafelanschrieb

Satz: Besitzt die Gleichung $ax + by = c$ eine Lösung $(x \mid y)$ mit $x, y \in \mathbb{Z}$, so folgt $\mathrm{ggT}(a, b) \mid c$.

Beweis: $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$
$\overset{\text{letzter Satz}}{\Rightarrow}$ $\mathrm{ggT}(a, b) \mid \underbrace{(ax + by)}_{=c}$. $\square$

Folgerung: Ist $\mathrm{ggT}(a, b)$ kein Teiler von c, so hat $ax + by = c$ keine ganzzahlige Lösung.

Anmerkung

Die Bedingung $\mathrm{ggT}(a, b) \mid c$ muss notwendigerweise erfüllt sein, damit die diophantische Gleichung $ax + by = c$ Lösungen besitzen kann. Diese Bedingung also ist eine *notwendige Bedingung* für die Lösbarkeit der Gleichung. Dass diese Bedingung auch hinreichend ist, werden wir erst in der nächsten Einheit klären.

Vorgehen: In den nächsten Aufgaben sollen die Schüler:innen jeweils die notwendige Bedingung für die Lösbarkeit überprüfen und eine Lösung erraten. Die Frage nach allen Lösungen wird erst später gestellt.

Weiter auf nächster Seite

Aufgabe 1.2 (*Arbeitsblatt 1.2 (Diophantische Gleichungen und ggT), Aufgabe 2*)

Gegeben sind diophantische Gleichungen der Form $ax + by = c$. Bestimme jeweils die Menge der gemeinsamen Teiler von a und b, den $\mathrm{ggT}(a, b)$ und untersuche, ob $\mathrm{ggT}(a, b)$ Teiler von c ist. Falls es Lösungen gibt, vereinfache die Gleichung, indem Du beide Seiten durch die selbe geeignet gewählte Zahl teilst und rate eine Lösung $(x \mid y)$.

a) $18x + 12y = 24$:

Menge der gemeinsamen Teiler von 18 und 12: $\{ \quad 1, 2, 3, 6 \quad \}$,

$\mathrm{ggT}(12, 18) =$ 6.

Die Gleichung ist

	nicht lösbar, denn
×	lösbar, denn ich habe eine Lösung gefunden: Vereinfachte Gleichung: $3x + 2y = 4$ Eine Lösung: $(x \mid y) =$ $(\ 0 \mid 2 \ )$

b) $45x + 30y = 5$:

Menge der gemeinsamen Teiler von 45 und 30: $\{ \quad 1, 3, 5, 15 \quad \}$,

$\mathrm{ggT}(45, 30) =$ 15.

Die Gleichung ist

×	nicht lösbar, denn 15 ist kein Teiler von $c = 5$
	lösbar, denn ich habe eine Lösung gefunden: Vereinfachte Gleichung: Eine Lösung: $(x \mid y) =$ $(\quad \mid \quad)$.

Datei: `Kryptographie11-DiophantischeGl-ggT`

Lösung: Ist bereits im Aufgabentext enthalten.
Weitere Lösungen zum Teil a): $(2 \mid -1)$, $(4 \mid -4)$, $(-2 \mid 5)$.

Aufgabe 1.3 (*Arbeitsblatt 1.2 (Diophantische Gleichungen und ggT), Zusatzaufgabe 1*)

Gegeben ist die diophantische Gleichung $300x + 468y = 108$. Fülle die Kästchen aus.

Menge der gemeinsamen Teiler von 300 und 468: $\{ \quad 1, 3, 4, 6, 12 \quad \}$,

$\mathrm{ggT}(300, 486) =$ 12.

Die Gleichung ist

	nicht lösbar, denn
×	lösbar, denn ich habe eine Lösung gefunden: Vereinfachte Gleichung: $25x + 39y = 9$ Eine Lösung: $(x \mid y) =$ $(-9 \mid 6 \ )$

Datei: `Kryptographie12-DiophantischeGl-ggT`

Lösung: Ist bereits im Aufgabentext enthalten. Weitere Lösung z.B. $(30 \mid -19)$.

Mündlich: Es ist ziemlich umständlich, immer alle gemeinsamen Teiler zweier Zahlen aufzuschreiben, um ihren ggT zu bestimmen. Wir lernen nun eine einfachere Methode kennen.

2.3 Euklidischer Algorithmus

Mündlich: Teilen mit Rest ist aus der Grundschule bekannt. Wie kann Teilen mit Rest als Formel aufgeschrieben werden, so dass man damit rechnen kann?

Tafelanschrieb

2. Der euklidische Algorithmus

Teilen mit Rest:

$13 : 4 = 3 \text{ R } 1$ bedeutet: $13 = 3 \cdot 4 + 1$

$223 : 25 = 8 \text{ R } 23$ bedeutet: $223 = 8 \cdot 25 + 23$

Satz (Teilen mit Rest): Seien $a, b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{N} = \{0, 1, \ldots\}$, so dass gilt:

$$a = kb + r \quad \text{und} \quad 0 \leq r \leq b - 1.$$

Anmerkung: Ohne die Bedingung $0 \leq r \leq b - 1$ sind k, r nicht eindeutig, z.B.

$$23 = 4 \cdot 5 + 3 \quad \text{und} \quad 23 = 3 \cdot 5 + 8.$$

> **Anmerkung**
> Ein Beweis ist nicht notwendig, denn die Gültigkeit ist offensichtlich. Für einen formalen Beweis siehe Kapitel 2.5.

Vorgehen: In der folgenden Aufgabe sollen alle Schüler:innen Teil a) lösen und dann eine weitere Teilaufgabe ihrer Wahl.

Aufgabe 1.4 (*Arbeitsblatt 1.3 (Teilen mit Rest), Aufgabe 3*)

Teile jeweils a durch b mit Rest und schreibe die Lösung als Gleichung $a = k \cdot b + r$ auf.

a) $a = 143,\ b = 12$: $a = 11b + 11$

b) $a = 14130,\ b = 58$: $a = 243b + 36$

Zusatzaufgaben:

c) $a = 1\,111\,111,\ b = 2\,222$: $a = 500b + 111$

d) $a = 123\,321,\ b = 2\,010$: $a = 61b + 711$

Hinweis: Teil a) geht im Kopf, aber für die anderen Aufgabenteile ist ein Taschrechner hilfreich.

Datei: `Kryptographie13-Teilen-mitRest`

Lösung: Ist bereits im Aufgabentext enthalten.

Mündlich: Durch mehrfaches Teilen mit Rest kann der ggT zweier Zahlen einfach berechnet werden. Wir sehen uns das in einem Beispiel an.

> **Anmerkung**
> Ein Algorithmus ist ein Rechenschema, mit dem ein Problemtyp in endlich vielen Rechenschritten gelöst werden kann. Auch die Lösungsformel für quadratische Gleichungen (sogenannte Mitternachtsformel) ist ein Algorithmus.

Tafelanschrieb

Euklidischer Algorithmus: Gesucht $\mathrm{ggT}(468, 60)$.

Teilen mit Rest:

$$\begin{aligned} 468 &= 7 \cdot 60 + 48 \\ 60 &= 1 \cdot 48 + 12 \\ 48 &= 4 \cdot \textcircled{12} \end{aligned} \qquad \Rightarrow \ \mathrm{ggT}(468, 60) = \textcircled{12}$$

Stimmt das immer?

Mündlich: Wir beweisen nun, dass dieser Algorithmus immer den ggT der zwei Zahlen liefert. Bevor wir das können, beweisen wir einen Satz, der offensichtlich sehr hilfreich dabei ist.

Tafelanschrieb

Satz: Sei $a = k \cdot b + r$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Beweis: 1) $\mathrm{ggT}(b, r)$ teilt b und r.

$\overset{\text{früherer Satz}}{\Rightarrow}$ $\mathrm{ggT}(b, r)$ teilt $a = k \cdot b + 1 \cdot r$

$\Rightarrow$ $\mathrm{ggT}(b, r)$ teilt a und b

$\Rightarrow$ $\mathrm{ggT}(b, r) \leq \mathrm{ggT}(a, b)$.

2) Löse die Gleichung nach r auf: $r = a - k \cdot b$.

Wie vorher folgt: $\mathrm{ggT}(a, b)$ teilt b und r

$\Rightarrow$ $\mathrm{ggT}(a, b) \leq \mathrm{ggT}(b, r)$.

1) und 2) $\Rightarrow$ $\mathrm{ggT}(b, r) = \mathrm{ggT}(a, b)$. $\square$

Euklidischer Algorithmus für $\mathrm{ggT}(98, 126)$:

$$\begin{aligned} \overbrace{126}^{a} &= 1 \cdot \overbrace{98}^{b} + \overbrace{28}^{r} && \overset{\text{Satz}}{\Rightarrow} && \mathrm{ggT}(\overbrace{126}^{a}, \overbrace{98}^{b}) &= \mathrm{ggT}(\overbrace{98}^{b}, \overbrace{28}^{r}) \\ 98 &= 3 \cdot 28 + 14 && \Rightarrow && \mathrm{ggT}(98, 28) &= \mathrm{ggT}(28, 14) \\ 28 &= 2 \cdot 14 && \Rightarrow && \mathrm{ggT}(28, 14) &= 14 \\ & && \Rightarrow && \mathrm{ggT}(126, 98) &= 14 \end{aligned}$$

Anmerkung

Hier reicht der Beweis am Beispiel.

Vorgehen: Bei der nächsten Aufgabe lösen alle Schüler:innen Teil a) und eine weitere Teilaufgabe ihrer Wahl. Wer noch Zeit hat, kann sich an die Zusatzaufgabe machen.

Aufgabe 1.5 (*Arbeitsblatt 1.4 (Euklidischer Algorithmus), Aufgabe 4*)

Berechne mit dem Euklidischen Algorithmus:

a) $\mathrm{ggT}(150, 54)$,

b) $\mathrm{ggT}(300, 468)$,

c) $\mathrm{ggT}(2717, 2431)$,

d) $\mathrm{ggT}(4263, 4641)$.

Datei: `Kryptographie14-EuklidischerAlgorithmus`

Lösung: **a)**
$$\begin{aligned} 150 &= 2\cdot 54 + 42 \\ 54 &= 1\cdot 42 + 12 \\ 42 &= 3\cdot 12 + 6 \\ 12 &= 2\cdot 6 \end{aligned} \quad \Rightarrow \ \mathrm{ggT}(150,54) = 6$$

b)
$$\begin{aligned} 468 &= 1\cdot 300 + 168 \\ 300 &= 1\cdot 168 + 132 \\ 168 &= 1\cdot 132 + 36 \\ 132 &= 3\cdot 36 + 24 \\ 36 &= 1\cdot 24 + 12 \\ 24 &= 2\cdot 12 \end{aligned} \quad \Rightarrow \ \mathrm{ggT}(300,468) = 12$$

c)
$$\begin{aligned} 2717 &= 1\cdot 2431 + 286 \\ 2431 &= 8\cdot 286 + 143 \\ 286 &= 2\cdot 143 \end{aligned} \quad \Rightarrow \ \mathrm{ggT}(2717,2431) = 143$$

d)
$$\begin{aligned} 4641 &= 1\cdot 4263 + 378 \\ 4263 &= 11\cdot 378 + 105 \\ 378 &= 3\cdot 105 + 63 \\ 105 &= 1\cdot 63 + 42 \\ 63 &= 1\cdot 42 + 21 \\ 42 &= 2\cdot 21 \end{aligned} \quad \Rightarrow \ \mathrm{ggT}(4263,4641) = 21$$

> **Anmerkung**
> Die Zusatzaufgabe rundet das erste Thema ab. Wie man alle Lösungen berechnet, wird jedoch erst in der zweiten Einheit untersucht.

Aufgabe 1.6 (*Arbeitsblatt 1.4 (Euklidischer Algorithmus), Zusatzaufgabe 2*)

Bestimme jeweils für die gegebene Gleichung $ax + y = c$ den größten gemeinsamen Teiler $\mathrm{ggT}(a,b)$. Vereinfache dann die gegebene Gleichung und suche möglichst viele verschiedene ganzzahlige Lösungen $(x \mid y)$. Kannst du ein Bildungsgesetz erkennen? Kannst Du eine Formel angeben, die alle Lösungen beschreibt?

a) $42x + 126y = 84$, **b)** $81x + 54y = 27$.

Datei: `Kryptographie15-DiophantischAlleLoesungen`

Lösung: **a)** $\mathrm{ggT}(42,126) = 42$, $42x + 126y = 84 \ \Leftrightarrow \ x + 3y = 2 \ \Leftrightarrow \ x = 2 - 3y$,

Alle Lösungen: $(x \mid y) = (2 - 3k \mid 0 + k)$ $(k \in \mathbb{Z})$

b) $\mathrm{ggT}(81,54) = 27$, $81x + 54y = 27 \ \Leftrightarrow \ 3x + 2y = 1$,

Alle Lösungen: $(x \mid y) = (1 + 2k \mid -1 - 3k)$ $(k \in \mathbb{Z})$.

2.4 Schriftliche Aufgaben (ohne Lösungen)

Aufgabe 1.7 (*Arbeitsblatt 1.8 (Schriftliche Aufgaben), Aufgabe 5*)

Wahr oder falsch? Kreuze an!

	wahr	falsch
Der größte gemeinsame Teiler zweier Zahlen kann 1 sein.		
Der größte gemeinsame Teiler zweier Zahlen kann 0 sein.		
Der größte gemeinsame Teiler zweier Zahlen kann negativ sein.		
Der größte gemeinsame Teiler zweier Zahlen a, b kann mit b übereinstimmen.		
Der größte gemeinsame Teiler zweier Zahlen a, b ist immer kleiner als a.		
Die Gleichung $4x + 6y = 1$ hat mindestens eine Lösung $(x \mid y)$ mit rationalen Zahlen x, y.		
Die Gleichung $4x + 6y = 1$ hat mindestens eine Lösung $(x \mid y)$ mit ganzen Zahlen x, y.		
Die Gleichung $2x + 7y = 1$ hat mindestens eine Lösung $(x \mid y)$ mit ganzen Zahlen x, y.		
Seien x, y, a, b ganze Zahlen, a, b nicht beide 0. Dann gilt: $\mathrm{ggT}(a, b) \mid (ax+by)$.		

Datei: `Kryptographie190-Wahr-Falsch`

Aufgabe 1.8 (*Arbeitsblatt 1.8 (Schriftliche Aufgaben), Aufgabe 6*)

Gegeben ist die Gleichung $4x+5y = 1$. Gib drei verschiedene Lösungen $(x \mid y)$ mit ganzen Zahlen x, y an.

Lösungen: $(x \mid y) = \boxed{\left(\quad \middle| \quad\right)}$, $\boxed{\left(\quad \middle| \quad\right)}$, $\boxed{\left(\quad \middle| \quad\right)}$.

Datei: `Kryptographie191-DiophantischeGleichung`

Weiter auf nächster Seite

Aufgabe 1.9 (*Arbeitsblatt 1.8 (Schriftliche Aufgaben), Aufgabe 7*)

Berechne den größten gemeinsamen Teiler der Zahlen 276 und 114 mit Hilfe des euklidischen Algorithmus.

Euklidischer Algorithmus:

$\Rightarrow\ \mathrm{ggT}(276, 114) =$

Datei: `Kryptographie192-EuklidAlgorithmus`

Aufgabe 1.10 (*Arbeitsblatt 1.8 (Schriftliche Aufgaben), Aufgabe 8*)

Gegeben ist die diophantische Gleichung

$$63x + 147y \ = \ 105. \qquad (*)$$

a) Bestimme den größten gemeinsamen Teiler von 63 und 147.

$\mathrm{ggT}(63, 147) =$

b) Dividiere die Gleichung $(*)$ auf beiden Seiten durch $\mathrm{ggT}(63, 147)$ und gibt die Gleichung an, die dadurch entsteht. Sie besitzt die selben Lösungen wie $(*)$.

Neue Gleichung: $(**)$

c) Errate zwei verschiedene Lösungen $(x \mid y)$ von $(**)$, wobei x, y ganze Zahlen sind.

Lösungen: $(x \mid y) = \left(\ \middle|\ \right)$, $\left(\ \middle|\ \right)$.

d) **Zusatzaufgabe:** Gib alle Lösungen $(x \mid y)$ mit ganzen Zahlen x, y von $(**)$ an.

Alle Lösungen: $(x \mid y) =$

Datei: `Kryptographie193-DiophantischeGl-ggT`

Weiter auf nächster Seite

2.5 Ergänzungen

Beweis zum Satz vom Teilen mit Rest:

Existenz: Setze $k := \max\{l \in \mathbb{N} : lb \leq a\}$ und $r := a - kb$

Dann folgt:
- $a = kb + r$
- $kb \leq a \;\Rightarrow\; r \geq 0$
- $(k+1)b \geq a+1 \;\Rightarrow\; -(k+1)b \leq -a-1$
  $\Rightarrow\; r = a-(k+1)b+b \leq a-a-1+b = b-1$
  $\Rightarrow\; r \leq b-1$

Eindeutigkeit: Sei $a = k'\,b + r'$ mit $0 \leq r' \leq b-1$
$\Rightarrow\; k'\,b \leq a$ und $(k'+1)b > a$
$\Rightarrow\; k' = \max\{l \in \mathbb{N} : lb \leq a\} = k$
Also $k' = k$ und damit auch $r' = r$. $\square$

3 Unterrichtseinheit 2: Diophantische Gleichungen

3.1 Vorbemerkungen

Ziele in diesem Kapitel:

- Kennenlernen des erweiterten euklidischen Algorithmus.
- Existenz von Lösungen diophantischer Gleichungen $ax + by = c$, wenn $\mathrm{ggT}(a, b)$ Teiler von c ist (Anwendung des erweiterten euklidischen Algorithmus).
- Eine Formel finden, die alle Lösungen einer diophantischen Gleichung beschreibt.

Mit Hilfe der Existenz von Lösungen können wir später beweisen, dass im endlichen Ring $\mathbb{Z}_m$, wenn m eine Primzahl ist, Division möglich ist (vgl. Seite 46). Mit Hilfe der Formel können wir dann Brüche in $\mathbb{Z}_m$ berechnen.

Auf die Einführung des kleinsten gemeinsamen Vielfachen wurde aus Zeitgründen verzichtet. Das kgV könnte bei der Formel für alle Lösungen einer linearen diophantischen Gleichung verwendet werden. Dann sollte man aber auch die Formel $a \cdot b = \mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b)$ beweisen.

3.2 Existenz von Lösungen

> **Anmerkung**
> Die Wiederholung möglichst kurz fassen.

Vorgehen: Schüler:innen schreiben nicht mit.

Tafelanschrieb

Wiederholung:

Diophantische Gleichung: $ax + by = c$
$a, b, c \in \mathbb{N}$ gegeben, ganzzahlige Lösung $(x \mid y)$ gesucht.

Satz: Ist $\mathrm{ggT}(a, b)$ kein Teiler von c, dann gibt es keine Lösung der Gleichung.

Mündlich: Wir wissen also, wann es keine ganzzahlige Lösung gibt. Heute klären wir, wann es ganzzahlige Lösungen gibt und wie man alle Lösungen berechnen kann.

Vorgehen: Zu Beginn der Doppelstunde wird eine diophantische Gleichung angeschrieben, deren Lösungen nicht einfach zu erraten sind. Im Verlauf der Stunde wird immer wieder diese Gleichung betrachtet.

Tafelanschrieb

3. Eine Lösung berechnen

Gesucht: Alle ganzzahligen Lösungen von $110x + 32y = 8$.

Mündlich: Bisher haben wir Lösungen erraten. Heute lernen wir eine Methode kennen, um Lösungen systematisch zu berechnen. Falls die Koeffizienten größere Zahlen sind, ist das unbedingt notwendig.

Als erstes betrachten wir diophantische Gleichungen mit spezieller rechter Seite.

Tafelanschrieb

Satz: Zu beliebig gewählten natürlichen Zahlen a, b gibt es ganze Zahlen x, y, so dass

$$ax + by \;=\; \mathrm{ggT}(a, b).$$

Mündlich: Wir machen uns an einem Beipiel klar, warum der Satz gilt. Dazu verwenden wir die Koeffizienten aus der ersten Gleichung. Außerdem sehen wir am Beispiel, wie man im allgemeinen Fall eine Lösung berechnet.

> **Anmerkung**
> Die linke Seite der Gleichung im nächsten Beispiel ist die selbe wie in der Gleichung, die zu Beginn der Einheit angeschrieben wurde.

Tafelanschrieb

Beispiel: Erweiterter Euklidischer Algorithmus für $110x + 32y \;=\; \mathrm{ggT}(110, 32)$.

Schritt 1:	Schritt 2:
$110 = 3 \cdot 32 + 14$	$14 = 110 - 3 \cdot 32$
$32 = 2 \cdot 14 + 4$	$4 = 32 - 2 \cdot 14$
$14 = 3 \cdot 4 \;\; + 2$	$2 = 14 - 3 \cdot 4$
$4 = 2 \cdot 2$	

$$\begin{aligned}
\Rightarrow\; \mathrm{ggT}(110, 32) \;=\; 2 &= 14 - 3(\overbrace{32 - 2 \cdot 14}^{4=}) \\
&= 14 - 3 \cdot 32 + 6 \cdot 14 \;=\; 7 \cdot 14 - 3 \cdot 32 \\
&= 7(\overbrace{110 - 3 \cdot 32}^{14=}) - 3 \cdot 32 \;=\; 7 \cdot 110 - 21 \cdot 32 - 3 \cdot 32 \\
&= 7 \cdot 110 - 24 \cdot 32
\end{aligned}$$

$\Rightarrow\; (x \mid y) = (7 \mid -24)$ ist eine Lösung.

Mündlich: Achtung: Die farbigen Zahlen dürfen nicht wegmultipliziert werden. Als Ergebnis wollen wir eine Zahl Mal 110 Minus oder Plus eine Zahl Mal 32 erhalten. Das bedeutet, dass die blau gefärbten Zahlen unbedingt stehen bleiben müssen.

Vorgehen: Zunächst wird der euklidische Algorithmus ganz normal durchgeführt (Schritt 1, Zeilen links vom Trennstrich, und die Folgerung $\mathrm{ggT}(110, 32) = 2$). Danach wird jede Zeile nach dem Rest aufgelöst (Schritt 2, rechts vom Trennstrich). Schließlich werden die Umformungen rechts vom ggT durchgeführt.

Mündlich: Wir sehen, dass diese Methode immer eine Lösung liefert. Auf einen allgemeinen Beweis können wir verzichten.

> **Anmerkung**
> Der verallgemeinerte euklidische Algorithmus kann auch ein bisschen anders aufgeschrieben werden, siehe Seite 26.

> **Anmerkung**
> In der nächsten Aufgabe entdecken die Schüler:innen, wie man vorgeht, wenn auf der rechten Seite der diophantischen Gleichung ein Vielfaches des $\mathrm{ggT}(a, b)$ steht. Dies wird dann im Anschluss allgemein an der Tafel vorgeführt und im Heft aufgeschrieben. So steht die Methode auch im Heft.

Aufgabe 2.1 (*Arbeitsblatt 2.1 (Eine Lösung berechnen), Aufgabe 1*)

Bestimme jeweils eine ganzzahlige Lösung $(x \mid y)$ der angegebenen Gleichung. Berechne dazu in den Aufgabenteilen a) und d) zunächst den ggT der Koeffizienten mit Hilfe des euklidischen Algorithmus. Erweitere dann den Algorithmus, um eine Lösung zu finden.

a) $96x + 66y = 6$,

b) $96x + 66y = 18$ (verwende hierzu die Lösung aus Teil a)),

c) Für beliebiges fest vorgegebenes $n \in \mathbb{N}$: $96x + 66y = n \cdot 6$ (auch hier erweist sich die Lösung aus Teil a) als nützlich),

d) **Zusatzaufgabe:** $119x + 143y = 1$,

e) **Zusatzaufgabe:** $119x + 143y = 4$.

Datei: `Kryptographie20-Loesung-mit-erweitertem-Euklid`

Lösung: **a)**

$$\begin{array}{rcl|rcl} 96 &=& 1\cdot 66 + 30 & 30 &=& 96 - 1\cdot 66 \\ 66 &=& 2\cdot 30 + 6 & 6 &=& 66 - 2\cdot 30 \\ 30 &=& 5\cdot 6 & & & \end{array}$$

$$\begin{array}{rcccl} \Rightarrow \ggT(96,66) &=& 6 &=& 66 - 2\cdot(96 - 1\cdot 66) \\ &=& 3\cdot 66 &-& 2\cdot 96 \end{array}$$

$\Rightarrow (x \mid y) = (-2 \mid 3)$

b) Die Lösung aus a) muss mit 3 multipliziert werden: $(x \mid y) = (-6 \mid 9)$.

c) Die Lösung aus a) muss mit n multipliziert werden: $(x \mid y) = (-2n \mid 3n)$.

d)

$$\begin{array}{rcl|rcl} 143 &=& 1\cdot 119 + 24 & 24 &=& 143 - 1\cdot 119 \\ 119 &=& 4\cdot 24 + 23 & 23 &=& 119 - 4\cdot 24 \\ 24 &=& 1\cdot 23 + 1 & 1 &=& 24 - 1\cdot 23 \\ 23 &=& 23\cdot 1 & & & \end{array}$$

$$\begin{array}{rcccl} \Rightarrow \ggT(143,119) &=& 1 &=& 24 - 1\cdot(119 - 4\cdot 24) \\ &=& 5\cdot 24 - 119 &=& 5\cdot(143 - 1\cdot 119) - 119 \\ &=& 5\cdot 143 - 6\cdot 119 & & \end{array}$$

$\Rightarrow 119\cdot(-6) + 143\cdot 5 = 1$. Also ist $(x \mid y) = (-6 \mid 5)$ eine Lösung.

e) Da die rechte Seite $= 4\cdot\ggT(119,143)$ ist, müssen die Zahlen aus d) noch mit 4 multipliziert werden (vgl. b), c)).

$\Rightarrow (x \mid y) = (-24 \mid 20)$

Mündlich: Wir haben nun gesehen, wie man im allgemeinen Fall, wenn die rechte Seite der diophantischen Gleichung ein n-faches von $\ggT(a,b)$ ist, eine Lösung bestimmen kann. Dies schreiben wir nun als Satz auf. Der Beweis funktioniert genauso, wie wir den Aufgabenteil c) in der letzten Aufgabe gelöst haben.

> **Anmerkung**
> Die Variable n im Teil c) der letzten Aufgabe kommt im Beweis wieder vor.

Tafelanschrieb

Satz: Seien $a, b, c \in \mathbb{N}$ gegeben, so dass $\mathrm{ggT}(a,b) \mid c$. Dann hat

$$ax + by \;=\; c \;=\; n \cdot \mathrm{ggT}(a,b)$$

mindestens eine ganzzahlige Lösung $(x \mid y)$.

Beweis: Es gibt ein $n \in \mathbb{N}$, so dass $c = n \cdot \mathrm{ggT}(a,b)$.

Letzter Satz $\Rightarrow$ es gibt ganzzahlige x, y mit

$ax + by \;=\; \mathrm{ggT}(a,b) \qquad \mid \cdot n$

$\Leftrightarrow\; n(ax+by) \;=\; n \cdot \mathrm{ggT}(a,b)$

$\Leftrightarrow\; a(nx) + b(ny) \;=\; c$

$\Rightarrow\; (nx \mid ny)$ ist ganzzahlige Lösung. $\square$

Mündlich: Mit der Methode, die im Beweis des Satzes verwendet wird, können wir nun immer eine Lösung berechnen, wenn eine Lösung existiert.

Vorgehen: Zur Erklärung, wie man eine Lösung berechnet, wird nun die Gleichung im Satz ergänzt durch die orange umkringelte Gleichheit, anschließend wird die Lösung $(nx \mid ny)$ orange umkringelt.

> **Anmerkung**
> Im nächsten Beispiel wird wieder die zu Beginn der Einheit angeschriebene Gleichung untersucht. $n = 4$ hat dieselbe Farbe wie im Beweis.

Tafelanschrieb

Beispiel: $110x + 32y = \mathrm{ggT}(110, 32) = 2$ hat die Lösung $(7 \mid -24)$.

$\Rightarrow\; 110x + 32y = 8 = 4 \cdot 2$ hat die Lösung $(4 \cdot 7 \mid 4 \cdot (-24)) = (28 \mid -96)$.

Mündlich: Wir wissen nun: Wenn der ggT von a, b die rechte Seite c teilt, dann gibt es mindestens eine ganzzahlige Lösung. Wenn der ggT von a, b die rechte Seite c nicht teilt, dann gibt es keine ganzzahlige Lösung.

3.3 Alle Lösungen finden

Mündlich: Wir wissen jetzt, wie man eine Lösung einer diophantischen Gleichung findet. Jetzt wollen wir alle Lösungen finden. Dazu gibt es nun Aufgaben, bei denen Ihr ausprobieren könnt, ob Ihr alle Lösungen findet.

Aufgabe 2.2 (*Arbeitsblatt 2.2 (Mehrere Lösungen finden), Aufgabe 2*)

Bestimme durch Probieren mehrere ganzzahlige Lösungen $(x \mid y)$, möglichst alle.

a) $3x + 2y = 1$: $(x \mid y) = (-1 \mid 2),\ (1 \mid -1),\ (3 \mid -4),\ (5 \mid -7),\ (7 \mid -10), \ldots$
oder allgemein: $(x \mid y) = (1 + 2k \mid -1 - 3k),\ k \in \mathbb{Z}$

Zusatzaufgabe:

b) $3x + 9y = 3$: $(x \mid y) = (1 \mid 0),\ (4 \mid -1),\ (7 \mid -2),\ (10 \mid -3), \ldots$
oder allgemein: $(x \mid y) = (1 + 3k \mid 0 - k),\ k \in \mathbb{Z}$

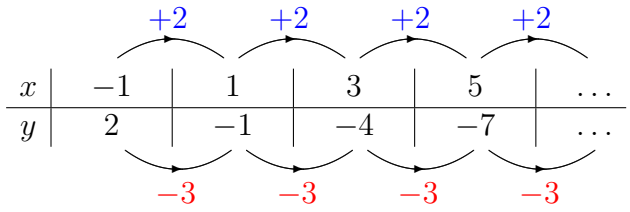
Datei: `Kryptographie21-Probieren-alleLoesungen`

Lösung: Ist bereits im Aufgabentext enthalten.

Tafelanschrieb

4. Alle Lösungen berechnen

Beobachtung: Die Gleichung $3x + 2y = 1$ hat die Lösungen



D.h. x wird in 2er Schritten erhöht und y in 3er Schritten erniedrigt.

Mündlich: Dieses Prinzip, dass x schrittweise um b erhöht wird, während y schrittweise um a erniedrigt wird, gilt allgemein. Wir schreiben dies als Satz auf.

Tafelanschrieb

Satz: 1) Ist $(x_0 \mid y_0)$ eine Lösung von $ax + by = c$, dann sind alle Zahlenpaare

$$(x \mid y) \;=\; (x_0 + k \cdot b \mid y_0 - k \cdot a) \text{ mit } k \in \mathbb{Z} \qquad (*)$$

ebenfalls Lösungen.

Mündlich: Die Variable k entspricht der Anzahl der Schritte, die wir oben nach rechts gehen.

Tafelanschrieb

2) Gilt $\mathrm{ggT}(a, b) = 1$, dann sind durch $(*)$ alle Lösungen gegeben.

Beweis: 1) Durch $(*)$ sind Lösungen gegeben, denn

$ax + by \;=\; a(x_0 + kb) + b(y_0 - ka) \;=\; ax_0 + \cancel{akb} + by_0 - \cancel{bka} \;=\; c.$

2) Sei $(x \mid y)$ irgendeine Lösung von $ax + by = c$.

Es gilt $a(x - x_0) + b(y - y_0) \;=\; ax + by - (ax_0 + by_0) \;=\; c - c \;=\; 0$

$\Rightarrow\; b(y - y_0) \;=\; -a(x - x_0).$

$\mathrm{ggT}(a, b) = 1 \;\Rightarrow\; b \mid (x - x_0) \;\Rightarrow\; x - x_0 = k \cdot b$ mit geeignetem $k \in \mathbb{Z}$.

$\Rightarrow\; y - y_0 \;=\; -\frac{a}{b}(x - x_0) \;=\; -\frac{a}{b} \cdot k \cdot b \;=\; -k \cdot a.$

$\Rightarrow\; y \;=\; y_0 - k \cdot a, \quad x \;=\; x_0 + k \cdot b$

$\Rightarrow\; (x \mid y)$ wird durch die Formel $(*)$ beschrieben. $\square$

Mündlich: Wir wenden nun die gefundene Formel auf die Gleichung aus unserem Beispiel an. Wir hatten bereits die Lösung $(28 \mid -96)$ gefunden.

Tafelanschrieb

Beispiel: $110\,x + 32\,y = 8 \qquad (1)$

hat die Lösung $(x_0 \mid y_0) = (28 \mid -96)$.

1) des Satzes: $(x \mid y) = (28 - k \cdot 32 \mid -96 + k \cdot 110)$ mit $k \in \mathbb{Z}$ sind Lösungen.

Mündlich: Dies sind jedoch nicht alle Lösungen.

Tafelanschrieb

Teile die Gleichung (1) auf beiden Seiten durch $2 = \mathrm{ggT}(110, 32)$:

$$55\,x + 16\,y \;=\; 4 \tag{2}$$

hat die selben Lösungen wie (1), und $\mathrm{ggT}(55, 16) = 1$.

2) des Satzes: Alle Lösungen von (2) sind

$$(x \mid y) = (28 + k \cdot 16 \mid -96 - k \cdot 55) \text{ mit } k \in \mathbb{Z}.$$

Dies sind auch alle Lösungen von (1).

Mündlich: Nun haben wir die diophantische Gleichung, die zu Beginn der Stunde angeschrieben wurde, vollständig gelöst.

> **Anmerkung**
> Es ist wichtig, dass die Schüler:innen zwei Dinge erkennen. Zum Einen, dass man die Gleichung durch $\mathrm{ggT}(a, b)$ teilen kann, und dass sich die Lösungsmenge dabei nicht ändert. Zum Anderen, dass die Formel aus dem letzten Satz erst dann alle Lösungen liefert, wenn man die Gleichung durch $\mathrm{ggT}(a, b)$ geteilt hat. Dazu dient auch die folgende Aufgabe.

Aufgabe 2.3 (*Arbeitsblatt 2.3 (Alle Lösungen bestimmen), Aufgabe 3*)

Gegeben ist die Gleichung

$$144x + 52y \;=\; 8. \tag{$*$}$$

a) Bestimme $\mathrm{ggT}(144, 52)$ mit Hilfe des euklidischen Algorithmus.

b) Erweitere den euklidischen Algorithmus und berechne eine ganzzahlige Lösung $(x \mid y)$ der Gleichung $144x + 52y = \mathrm{ggT}(144, 52)$.

c) Berechne eine Lösung von $(*)$.

d) Teile die Gleichung $(*)$ auf beiden Seiten durch $\mathrm{ggT}(144, 52)$ und gib die Gleichung an, die dadurch ensteht.

e) Gib alle ganzzahligen Lösungen von $(*)$ an.

Datei: `Kryptographie26-AlleLoesungen-mitAnleitung`

Lösung: **a)** und **b)**

$$\begin{array}{rcl|rcl} 144 &=& 2 \cdot 52 + 40 & 40 &=& 144 - 2 \cdot 52 \\ 52 &=& 1 \cdot 40 + 12 & 12 &=& 52 - 40 \\ 40 &=& 3 \cdot 12 + 4 & 4 &=& 40 - 3 \cdot 12 \\ 12 &=& 3 \cdot 4 & & & \end{array}$$

$$\begin{aligned} \mathrm{ggT}(144, 52) = 4 &= 40 - 3(52 - 40) \\ &= 4 \cdot 40 - 3 \cdot 52 \\ &= 4(144 - 2 \cdot 52) - 3 \cdot 52 \\ &= 4 \cdot 144 - 11 \cdot 52 \end{aligned}$$

$\Rightarrow$ $(x \mid y) = (4 \mid -11)$ ist eine Lösung von $144x + 52y = 4 = \mathrm{ggT}(144, 52)$

b) $8 = 2 \cdot \mathrm{ggT}(144, 52) \;\Rightarrow\; (x \mid y) = (2 \cdot 4 \mid 2 \cdot (-11)) = (8 \mid -22)$ ist eine Lösung.

c) $36x + 13y = 2$.

d) $(x \mid y) = (8 + k \cdot 13 \mid -22 - k \cdot 36)$ mit $k \in \mathbb{Z}$.

Mündlich: Wir können also feststellen, ob eine lineare diophantische Gleichung Lösungen besitzt. Und falls Lösungen existieren, können wir alle berechnen bzw. angeben.

> **Anmerkung**
> Die folgende Aufgabe zeigt deutlich, dass wir nun viel mehr wissen als zu Beginn dieser Einheit.
>
> Dadurch, dass aus Aufgabe 1 jeweils bereits eine Lösung bekannt ist, kann hier auf den euklidischen Algorithmus verzichtet werden. Es muss nur die Aussage des letzten Satzes angewandt werden. Und der Aufgabenteil c) zeigt sehr deutlich, welcher Teil der Lösung mit dem Faktor $n = \frac{c}{\mathrm{ggT}(a,b)}$ multipliziert werden muss.

Vorgehen: Die Lösungen zur folgenden Aufgabe werden als Lösungsblatt zur Verfügung gestellt, siehe Kapitel 12, Lösungsblatt nach dem Aufgabenblatt 3.

Aufgabe 2.4 (*Arbeitsblatt 2.3 (Zusatzaufgaben), Aufgabe 4*)

Bestimme alle Lösungen für die Gleichungen aus Aufgabe 1 dieser Einheit (siehe Arbeitsblatt 1).

a) $96x + 66y = 6$,

b) $96x + 66y = 18$,

c) Für beliebiges fest vorgegebenes $n \in \mathbb{N}$: $96x + 66y = n \cdot 6$,

d) Zusatzaufgabe: $119x + 143y = 1$,

e) Zusatzaufgabe: $119x + 143y = 4$.

Datei: `Kryptographie22-AlleLoesungenAufgabe1`

Lösung: **a)** Aus der Aufgabe 1a ist bekannt: Eine Lösung ist $(x \mid y) = (-2 \mid 3)$. Teile die Gleichung durch $\mathrm{ggT}(96, 66) = 6$:

$$96x + 66y = 6 \;\Leftrightarrow\; 16x + 11y = 1.$$

Wegen $\mathrm{ggT}(16, 11) = 1$ sind nach dem letzten Satz alle Lösungen gegeben durch

$$(x \mid y) \;=\; (-2 + 11k \mid 3 - 16k), \quad (k \in \mathbb{Z}).$$

b) Genauso: Eine Lösung ist $(x \mid y) = (-6 \mid 9)$. Teile die Gleichung durch 6: $16x + 11y = 3$. Alle Lösungen:

$$(x \mid y) \;=\; (-6 + 11k \mid 9 - 16k), \quad (k \in \mathbb{Z}).$$

Beachte, dass nur der Teil der Lösung aus Teil a), der nicht den Faktor k enthält, mit 3 multipliziert wird!

c) Genauso: Alle Lösungen $(x \mid y) = (-2n + 11k \mid 3n - 16k)$, $(k \in \mathbb{Z})$.

d) Wegen $\mathrm{ggT}(143, 119) = 1$ sind bereits die Voraussetzungen des letzten Satzes erfüllt. Eine Lösung ist $(x \mid y) = (-6 \mid 5)$.

$\Rightarrow$ $(x \mid y) = (-6 + 143k \mid 5 - 119k)$ mit $k \in \mathbb{Z}$ sind alle Lösungen.

e) Alle Lösungen sind $(x \mid y) = (-24 + 143k \mid 20 - 119k)$ mit $k \in \mathbb{Z}$.

3.4 Schriftliche Aufgaben (ohne Lösungen)

Aufgabe 2.5 (*Arbeitsblatt 2.4 (Schriftliche Aufgaben), Aufgabe 5*)

Wahr oder falsch? Kreuze an!

	wahr	falsch
Die diophantische Gleichung $ax+by=c$ besitzt entweder keine oder unendlich viele ganzzahlige Lösungen $(x \mid y)$.		
Gilt $\mathrm{ggT}(a,b) \mid c$, dann hat die Gleichung $ax+by=c$ genau eine ganzzahlige Lösung $(x \mid y)$.		
Gilt $\mathrm{ggT}(a,b) \mid c$, dann hat die Gleichung $ax+by=c$ unendlich viele ganzzahlige Lösungen $(x \mid y)$.		
Hat die diophantische Gleichung $ax+by=c$ mindestens eine ganzzahlige Lösung $(x \mid y)$, so folgt $\mathrm{ggT}(a,b) \mid c$.		
Mit dem erweiterten euklidischen Algorithmus berechnet man eine ganzzahlige Lösung $(x \mid y)$ von $ax+by=\mathrm{ggT}(a,b)$.		
Mit dem erweiterten euklidischen Algorithmus berechnet man alle ganzzahligen Lösungen $(x \mid y)$ von $ax+by=\mathrm{ggT}(a,b)$.		
Ist $(x_0 \mid y_0)$ eine ganzzahlige Lösung von $ax+by=c$, so sind alle Lösungen durch $(x_0+kb \mid y_0-ka)$ mit $k \in \mathbb{Z}$ gegeben.		
Ist $(x_0 \mid y_0)$ eine ganzzahlige Lösung von $ax+by=\mathrm{ggT}(a,b)$, so ist $(x \mid y)=(5x_0 \mid 5y_0)$ eine Lösung von $ax+by=5\mathrm{ggT}(a,b)$.		

Datei: `Kryptographie290-Wahr-Falsch`

Aufgabe 2.6 (*Arbeitsblatt 2.4 (Schriftliche Aufgaben), Aufgabe 6*)

Gegeben ist die diophantische Gleichung

$$71x+43y \;=\; 2. \qquad (*)$$

a) Die Zahlen $a=71$ und $b=43$ sind Primzahlen. Gib den größten gemeinsamen Teiler an.

$\mathrm{ggT}(71,43) =$ ☐.

b) Warum ist $(x \mid y)=(-3 \mid 5)$ eine Lösung von $(*)$?

☐

c) Gib alle Lösungen der Gleichung $(*)$ an.

Alle Lösungen $(x \mid y) =$ ☐.

d) Gib alle Lösungen der Gleichung $71x+43y=8$ an.

Alle Lösungen $(x \mid y) =$ ☐.

Datei: `Kryptographie292-AlleLoesungen`

Aufgabe 2.7 (*Arbeitsblatt 2.4 (Schriftliche Aufgaben), Aufgabe 7*)

Gegeben ist die diophantische Gleichung

$$108x + 300y \;=\; 60. \qquad (*)$$

a) Führe den erweiterten euklidischen Algorithmus durch, um $\mathrm{ggT}(108, 300)$ und eine ganzzahlige Lösung $(x \mid y)$ der Gleichung $108x + 300y = \mathrm{ggT}(108, 300)$ zu erhalten.

Schritt 1:

Schritt 2:

$\mathrm{ggT}(108, 300) =$

Eine Lösung der Gleichung $108x + 300y = \mathrm{ggT}(108, 300)$: $(x \mid y) =$.

b) Gib eine Lösung von $(*)$ an. Lösung: $(x \mid y) =$.

c) Vereinfache die Gleichung $(*)$, indem Du sie durch eine möglichst große Zahl teilst.

Vereinfachte Gleichung: .

Für die Lösungen von $(*)$ und die Lösungen der vereinfachten Gleichung gilt:

.

d) Gib alle Lösungen von $(*)$ an.

Alle Lösungen von $(*)$: $(x \mid y) =$.

Datei: `Kryptographie291-ErweiterterEuklid`

3.5 Weitere Aufgaben

Aufgabe 2.8 (*Arbeitsblatt 2.5 (Zusatzaufgaben), Aufgabe 8*)

Bestimme alle Lösungen der Gleichung $144x + 400y = 48$.

Datei: `Kryptographie23-AlleLoesungenSystematisch`

Lösung:

$$\begin{array}{rcl|rcl} 400 &=& 2\cdot 144 + 112 & 112 &=& 400 - 2\cdot 144 \\ 144 &=& 1\cdot 112 + 32 & 32 &=& 144 - 1\cdot 112 \\ 112 &=& 3\cdot 32 + 16 & 16 &=& 112 - 3\cdot 32 \\ 32 &=& 2\cdot 16 & &=& 112 - 3\cdot(144 - 1\cdot 112) \;=\; 4\cdot 112 - 3\cdot 144 \\ & & & &=& 4\cdot(400 - 2\cdot 144) - 3\cdot 144 \end{array}$$

$$\Rightarrow\ \mathrm{ggT}(400, 144) \;=\; 16 \;=\; 144\cdot(-11) + 400\cdot 4$$

Also ist eine Lösung: $(x \mid y) = (3\cdot(-11) \mid 3\cdot 4) = (-33 \mid 12)$.

Alle Lösungen: Teile die Gleichung durch $\mathrm{ggT}(144, 400) = 16$:

$$144x + 400y = 48 \;\Leftrightarrow\; 9x + 25y = 3.$$

$\Rightarrow\ (x \mid y) = (-33 + 25k \mid 12 - 9k)$, $k \in \mathbb{Z}$ sind alle Lösungen.

Eine einfachere Darstellung der Lösungen ergibt sich, wenn man die Lösung mit $k = 1$ zugrunde legt: $(x \mid y) = (-8 + 25k \mid 3 - 9k)$, $k \in \mathbb{Z}$.

Aufgabe 2.9 (*Arbeitsblatt 2.5 (Zusatzaufgaben), Aufgabe 9*)

Ein zerstreuter Bankkassierer verwechselte 1-Euromünzen und 1-Centmünzen, als er den Scheck von Herrn Krause auszahlte, indem er ihm 1-Euromünzen anstelle von 1-Centmünzen und 1-Centmünzen anstelle von 1-Euromünzen gab. Nachdem Herr Krause zuhause großzügig 5 Cent in die Spardose seines Sohnes getan hatte, entdeckte er, dass er jetzt noch genau doppelt so viel Geld hatte, wie auf dem Scheck stand. Auf welche Summe war der Scheck ausgestellt?

Datei: `Kryptographie24-ZerstreuterKassier`

Lösung: Es seien x die Anzahl der **ausgezahlten** Euromünzen, y die Anzahl der ausgezahlten Centmünzen. Somit hat Herr Krause die Summe $S = 100x + y$ Cent erhalten. Da beim Auszahlen Euro und Cent verwechselt wurden, ist der Scheck auf den Betrag $B = 100y + x$ Cent ausgestellt. Die Bedingung $S - 5 = 2B$ führt auf die Gleichung

$$100x + y - 5 \;=\; 2(100y + x)$$

bzw.

$$98x - 199y \;=\; 5. \qquad (*)$$

$$\begin{array}{rl|l} 199 = 2\cdot 98 + 3 & 3 &= 199 - 2\cdot 98 \\ 98 = 32\cdot 3 + 2 & 2 &= 98 - 32\cdot 3 \\ 3 = 1\cdot 2 + 1 & 1 = 3 - 2 &= 3 - (98 - 32\cdot 3) \;=\; 33\cdot 3 - 98 \\ & &= 33(199 - 2\cdot 98) - 98 \;=\; 33\cdot 199 - 67\cdot 98 \end{array}$$

$$\Rightarrow\quad \mathrm{ggT}(199, 98) \;=\; 1 \;=\; 33\cdot 199 - 67\cdot 98$$

Die letzte Gleichung muss mit 5 multipliziert werden. Alle Lösungen von $(*)$ sind durch

$$(x \mid y) \;=\; (-335 + k\cdot 199 \mid -165 + k\cdot 98) \quad \text{mit } k \in \mathbb{Z}$$

gegeben. Nun ist die Lösung gesucht, für die $0 \leq x \leq 99$ gilt. Damit muss $k = 2$ gewählt werden:

$$(x \mid y) \;=\; (-335 + 2 \cdot 199 \mid -165 + 2 \cdot 98) \;=\; (63 \mid 31).$$

Somit hat Herr Krause den Betrag 63 Euro und 31 Cent ausgezahlt bekommen. Diese Lösung ist eindeutig, da andere Wahlen von k auf Cent-Beträge größer gleich 100 führen. Der Scheck war auf den Betrag 31 Euro 63 Cent ausgestellt.

Aufgabe 2.10 (*Arbeitsblatt 2.5 (Zusatzaufgaben), Aufgabe 10*)

Gib alle natürlichen Zahlen an, die bei Division durch 19 den Rest 3 und gleichzeitig bei Division durch 29 den Rest 18 lassen.

Hinweis: Die erste Bedingung lässt sich als Gleichung $x = k \cdot 19 + 3$ formulieren, entsprechend die zweite Bedingung als $x = -l \cdot 29 + 18$ (mit negativem l). Eliminiere zunächst x und löse die entstehende diophantische Gleichung. Beachte, dass nur natürliche Zahlen gesucht sind.

Datei: `Kryptographie25-Reste-beiDivision`

Lösung: $x = 19k + 3 \wedge x = -29l + 18$

Gleichsetzen $\Rightarrow\; 19k + 3 = -29l + 18 \;\Leftrightarrow\; 19k + 29l = 15$

$$\begin{array}{l|l} 29 = 1 \cdot 19 + 10 & 10 = 29 - 19 \\ 19 = 1 \cdot 10 + \;\; 9 & \;\; 9 = 19 - 10 \\ 10 = 1 \cdot 9 \;\; + \;\; 1 & \;\; 1 = 10 - 9 \;=\; 10 - (19 - 10) \end{array}$$

$$= 2 \cdot 10 - 19 \;=\; 2(29 - 19) - 19$$

$$\Rightarrow \quad \mathrm{ggT}(29, 19) \;=\; 1 \;=\; 2 \cdot 29 - 3 \cdot 19$$

Eine Lösung der diophantischen Gleichung ist damit $(k \mid l) = (-45 \mid 30)$, alle Lösungen sind durch

$$(k \mid l) \;=\; (-45 + t \cdot 29 \mid 30 - t \cdot 19) \quad \text{mit } t \in \mathbb{Z}$$

gegeben.

Wir suchen nun positive Zahlen der Form $x = k \cdot 19 + 3$. Das kleinste positive k, das in der letzten Gleichung auftritt, ist $k = -45 + 2 \cdot 29 = 13$. Damit sind alle gesuchten Zahlen gegeben durch

$$x = (13 + m \cdot 29) \cdot 19 + 3 = 250 + m \cdot 551 \text{ mit } m = 0, 1, 2, \ldots \;.$$

Aufgabe 2.11 (*Arbeitsblatt 2.5 (Zusatzaufgaben), Aufgabe 11*)

Gegeben sind zwei natürliche Zahlen a, b mit den Darstellungen

$$a \;=\; p_1^3 \cdot p_2 \cdot p_3^4, \quad b \;=\; p_1^2 \cdot p_3 \cdot p_4^2,$$

wobei $p_1, \ldots, p_4$ paarweise verschiedene Primzahlen sind. Man nennt diese Darstellung **Primfaktorzerlegung**.

a) Wie kann man aus dieser Darstellung $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ ausrechnen?

b) Wie hängen $a \cdot b$, $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ zusammen?

Datei: `Kryptographie27-ggT-kgV-Primfaktorzerlegung`

Lösung: **a)** $\mathrm{ggT}(a, b) = p_1^2 \cdot p_3$, $\mathrm{kgV}(a, b) = p_1^3 \cdot p_2 \cdot p_3^4 \cdot p_4^2$

b) $a \cdot b = p_1^5 \cdot p_2 \cdot p_3^5 \cdot p_4^2$.
Es gilt $\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = a \cdot b$.

3.6 Ergänzungen

Andere Schreibweise für den erweiterten euklidischen Algorithmus:
Der verallgemeinerte euklidische Algorithmus kann auch folgendermaßen aufgeschrieben werden:

Erweiterter Euklidischer Algorithmus für $110x + 32y \;=\; \mathrm{ggT}(110, 32)$.

Schritt 1:	Schritt 2:
$110 = 3 \cdot 32 + 14$	$14 = 110 - 3 \cdot 32$
$32 = 2 \cdot 14 + 4$	$4 = 32 - 2 \cdot 14 = 32 - 2(110 - 3 \cdot 32) = 7 \cdot 32 - 2 \cdot 110$
$14 = 3 \cdot 4 + 2$	$2 = 14 - 3 \cdot 4 = 110 - 3 \cdot 32 - 3(7 \cdot 32 - 2 \cdot 110) = 7 \cdot 110 - 24 \cdot 32$
$4 = 2 \cdot 2$	

$\Rightarrow \; \mathrm{ggT}(110, 32) = 2 = 110 \cdot 7 + 32 \cdot (-24)$.

Hier wird im Schritt 2 in jeder Gleichung direkt eine ganzzahlige Linearkombination der zugrunde liegenden Zahlen erzeugt. Das kann übersichtlicher sein, denn man hat immer vor Augen, dass eine ganzzahlige Linearkombination von 110 und 32 gesucht wird.

Der folgende Satz wurde aus Zeitgründen im Schülerseminar weggelassen. Er bringt auch keinen Fortschritt, nur eine Formel, die die bisherige Methode zusammenfasst.

Satz: Ist $(x_0 \mid y_0)$ eine Lösung von $ax + by = c$, dann sind alle Lösungen durch

$$(x \mid y) \;=\; \Big(x_0 + k \underbrace{\frac{b}{\mathrm{ggT}(a,b)}}_{=:b'} \;\Big|\; y_0 - k \underbrace{\frac{a}{\mathrm{ggT}(a,b)}}_{=:a'}\Big) \quad (k \in \mathbb{Z})$$

gegeben.

Beweis: Teilen durch $\mathrm{ggT}(a, b)$:

$$\begin{aligned} & ax + by \;=\; c && (*) \\ \Leftrightarrow \quad & \underbrace{\frac{a}{\mathrm{ggT}(a,b)}}_{=a'} x + \underbrace{\frac{b}{\mathrm{ggT}(a,b)}}_{=b'} y \;=\; \underbrace{\frac{c}{\mathrm{ggT}(a,b)}}_{=:c'} && \\ \Leftrightarrow \quad & a'x + b'y \;=\; c' && (**) \end{aligned}$$

Beachte: $\mathrm{ggT}(a, b) \mid a, b \;\Rightarrow\; a', b' \in \mathbb{N}$.

Es gibt eine Lösung von $(*) \;\Rightarrow\; \mathrm{ggT}(a, b) \mid c \;\Rightarrow c' \in \mathbb{N}$.

Außerdem: $\mathrm{ggT}(a', b') = 1$.

$(x_0 \mid y_0)$ ist Lösung von $(*) \;\Leftrightarrow\; (x_0 \mid y_0)$ ist Lösung von $(**)$

Letzter Satz $\Rightarrow$ $(x_0 + kb' \mid y_0 - ka')$ sind alle Lösungen von $(**)$

$\Leftrightarrow$ $(x_0 + kb' \mid y_0 - ka')$ sind alle Lösungen von $(*)$ $\square$

4 Unterrichtseinheit 3: Kongruenzen

4.1 Vorbemerkungen

In dieser und der folgenden Doppelstunde werden Restklassenringe eingeführt. Dieses Thema ist zunächst unabhängig von den vorigen Einheiten. Erst am Ende der nächsten Doppelstunde wird die Lösungstheorie für diophantische Gleichungen benötigt, um die Existenz von Brüchen in Primzahl-Restklassenringen zu beweisen.

Die Idee für diese Einheit besteht darin, am Anfang und am Ende die Quersummenregel für die Teilbarkeit durch 9 zu thematisieren. Zu Beginn die Regel, am Schluss den Beweis der Regel.

Eine Wiederholung entfällt, da diese Einheit unabhängig von den ersten zwei Einheiten ist.

Hinweis: Die letzte der schriftlichen Aufgaben ist schwieriger als die bisherigen schriftlichen Aufgaben.

4.2 Teilbarkeit durch 9

> **Anmerkung**
> In der folgenden Aufgabe können Schüler:innen die Quersummenregel entdecken, falls sie diese noch nicht kennen. Deshalb wurden bei b) und c) bzw. bei d) und e) nur die Ziffern permutiert.
>
> Achtung: Die Lösungen der Aufgabenteile b) und c) werden später benötigt.

Aufgabe 3.1 (*Arbeitsblatt 3.1 (Teilen durch 9), Aufgabe 1*)

Bestimme den Rest beim Teilen durch 9.

a) 1000: $R = 1$ **b)** 2005: $R = 7$ **c)** 2050: $R = 7$

d) 1035: $R = 0$ **e)** 5103: $R = 0$

Datei: `Kryptographie30-TeilenDurch9`

Lösung: Ist bereits im Aufgabentext enthalten.

Aufgabe 3.2 (*Arbeitsblatt 3.1 (Teilen durch 9), Zusatzaufgabe 1*)

Bestimme eine vierstellige, eine fünfstellige und eine sechsstellige Zahl, die beim Teilen durch 9 den Rest 3 lassen.

Datei: `Kryptographie36-TeilenDurch9rueckwaerts`

Lösung: Z.B. $1\,002 = 999 + 3$, $10\,002 = 9\,999 + 3$, $100\,002 = 99\,999 + 3$.

Mündlich: Vermutung: Die Quersumme hat etwas mit dem Rest beim Teilen durch 9 zu tun. Wir testen an zwei Zahlen.

Vorgehen: Schüler:innen schreiben nicht mit.

Tafelanschrieb

$34:$ Quersumme $= 7$, $34 : 9 = 3\text{R}7$

$349:$ QS $= 16$, $349 : 9 = 38\text{R}7$

$$\begin{array}{r} -\ 27 \\ \hline 79 \\ -72 \\ \hline 7 \end{array}$$

Mündlich: Im zweiten Fall stimmen R und die Quersumme nicht überein. Schüler:innen fragen, was sie davon halten.

4.3 Kongruenzen

Tafelanschrieb

5. Kongruenzen

Mündlich: Was sind Kongruenzen? Kongruente Dreiecke?

Kongruente Dreiecke sind deckungsgleich, aber nicht identisch.

Hier geht es jedoch um Kongruenz von Zahlen.

Tafelanschrieb

Definition: Seien a, b ganze Zahlen, $m \in \mathbb{N}_+ = \{1, 2, \ldots\}$. Schreibe

$$a \equiv b \mod m \qquad (a \text{ ist kongruent zu } b \text{ modulo } m),$$

falls $a - b$ durch m teilbar ist.

Beispiel: $15 \equiv 3 \mod 6$, denn $15 - 3 = 12$ ist durch 6 teilbar.

> **Anmerkung**
> Schülerfrage: Hat dieses *kongruent* etwas mit der Kongruenz von Dreiecken zu tun?
> Mögliche Antwort: Beide sind Kongruenzrelationen. Kongruenzrelationen beschreiben Objekte, die in gewissen Eigenschaften übereinstimmen, obwohl sie nicht identisch sind.
> Oder: Nicht direkt. Aber in der Mathematik bezeichnet man Objekte als kongruent, die in bestimmten Eigenschaften übereinstimmen, aber verschieden sind. Je nach Zusammenhang gibt es verschiedene Kongruenzbegriffe.

Mündlich: Wir formulieren die Bedingung für „kongruent modulo m“ um. Dazu schreiben wir einen Satz auf.

Tafelanschrieb

Satz (Kongruenzkriterien): Folgende Aussagen sind äquivalent:

(1) $a \equiv b \mod m$
(2) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$
(3) a und b lassen beim Teilen durch m den selben Rest.

Mündlich: „Äquivalent“ bedeutet, dass alle drei Aussagen gleichzeitig wahr bzw. gleichzeitig falsch sind.

Wir haben also drei Möglichkeiten, eine Kongruenz nachzuweisen. Die Definition, also dass $a-b$ durch m teilbar ist, oder die Bedingung (2) oder (3).

Wir sehen, dass Kongruenz eine Abschwächung der Gleichheit von Zahlen ist. Wenn zwei Zahlen gleich sind, dann sind sie kongruent modulo m. Umgekehrt gilt das nicht, wie wir am Beispiel oben sehen. Zwei Zahlen sind schon dann kongruent, wenn der Rest beim Teilen durch m gleich ist.

Tafelanschrieb

Beweisprinzip Ringschluss:

$$\begin{array}{ccc} & (1) & \\ \nearrow & & \searrow \\ (3) & \Longleftarrow & (2) \end{array}$$

Mündlich: Wenn (1) wahr ist, dann ist auch (2) wahr, und dann ist auch (3) wahr.
Wenn (2) wahr ist, dann ist auch (3) wahr und dann auch (1).

Anmerkung
Der Ringschluss darf nicht mit dem *Zirkelschluss* verwechselt werden, der eine falsche Schlussweise bezeichnet.

Tafelanschrieb

Beweis: (1) $\Rightarrow$ (2):

$$\begin{aligned} a \equiv b \mod m &\Leftrightarrow m \mid (a-b) \\ &\Rightarrow \text{Es gibt ein } k \in \mathbb{Z}, \text{ so dass } a-b = k\cdot m \quad \big| +b \\ &\Rightarrow a = km+b = b+km \end{aligned}$$

(2) $\Rightarrow$ (3): Sei r der Rest beim Teilen von b durch m,
d.h. $b = lm + r$ mit einem $l \in \mathbb{Z}$.

$$\begin{aligned} (2) \Rightarrow a &= b+km \\ &= lm+r+km \\ &= \underbrace{(l+k)}_{\in\mathbb{Z}} m + r \end{aligned}$$

$\Rightarrow$ a lässt beim Teilen durch m den selben Rest r wie b.

(3) $\Rightarrow$ (1): $a = km+r,\ b = lm+r$ mit $k,l \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow\ a-b &= km+r-(lm+r) \\ &= km+\cancel{r}-kl-\cancel{r} \\ &= (k-l)m \\ \Rightarrow\ & m \mid (a-b) \\ \Leftrightarrow\ & a \equiv b \mod m \end{aligned}$$

□

Aus Aufgabe 1: b) $2005 : 9 = 222$ R 7
$\Leftrightarrow 2005 = 9\cdot 222 + 7$
$\Rightarrow 2005 \equiv 7 \mod 9$

c) $2050 \equiv 7 \mod 9$
$\Rightarrow 2050 \equiv 2005 \mod 9$

Anmerkung
Mit den Aufgaben auf dem nächsten Übungsblatt sollen die Kenntnisse zum *Teilen mit Rest* wieder aktiviert und der Umgang mit Kongruenzen und den äquivalenten Bedingungen durch Umkehraufgaben geübt werden.

Aufgabe 3.3 (*Arbeitsblatt 3.2 (Kongruenzgleichungen), Aufgabe 2*)

Bestimme jeweils das Ergebnis beim Teilen mit Rest. Trage Deine Lösungen in die Kästchen ein.

a) $33 = \boxed{5} \cdot 6 + \boxed{3}$

$\Rightarrow 33 \equiv \boxed{3} \mod 6$

b) $-101 = \boxed{-26} \cdot 4 + \boxed{3}$

$\Rightarrow -101 \equiv \boxed{3} \mod 4$

Datei: `Kryptographie31-Kongruenzen-einfach`

Lösung: Bereits im Aufgabentext enthalten.

Aufgabe 3.4 (*Arbeitsblatt 3.2 (Kongruenzgleichungen), Aufgabe 3*)

Bestimme möglichst alle ganzzahligen Lösungen x der folgenden Gleichungen.

a) $5 + x \equiv 2 \mod 7$: $L = \{\ldots, -10, -3, 4, 11, \ldots\}$
$= \{4 + 7k \text{ mit beliebigem } k \in \mathbb{Z}\}$

b) $5 \cdot x \equiv 2 \mod 7$: $L = \{\ldots, -8, -1, 6, 13, \ldots\}$
$= \{6 + 7k \text{ mit beliebigem } k \in \mathbb{Z}\}$

Datei: `Kryptographie32-Kongruenzgleichungen`

Lösung: Ist bereits im Aufgabentext enthalten.

Aufgabe 3.5 (*Arbeitsblatt 3.2 (Kongruenzgleichungen), Zusatzaufgabe 2*)

Bestimme möglichst alle ganzzahligen Lösungen x der folgenden Gleichungen.

a) $5 \cdot x \equiv 2 \mod 10$: Die Gleichung ist nicht lösbar, da $5 \cdot x \equiv 0 \mod 10$ für gerades x und $5 \cdot x \equiv 5 \mod 10$ für ungerades x

b) $-34 \equiv x \mod 5$: $L = \{\ldots -34, -29, \ldots, -4, 1, 6, \ldots\}$
$= \{1 + 5k \text{ mit beliebigem } k \in \mathbb{Z}\}$

Datei: `Kryptographie33-Kongruenzgleichungen`

Lösung: Ist bereits im Aufgabentext enthalten.

4.4 Rechenregeln für Kongruenzen

Tafelanschrieb

Satz (Rechenregeln für Kongruenzen):

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann:

$a_1)$ $-a \equiv -b \mod m$

$a_2)$ $a + c \equiv b + d \mod m$

$a_3)$ $ac \equiv bd \mod m$

$a_4)$ $a^2 \equiv b^2 \mod m$, $a^3 \equiv b^3 \mod m$, $\ldots$

Mündlich: Die Rechenoperationen Plus und Mal vertragen sich mit der Kongruenz. Das ist genau so, wie man es von der Gleichheit von Zahlen kennt (oder wie man es erwartet).

Tafelanschrieb

b) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann

$b_1)$ $a \equiv a \mod m$
$b_2)$ $b \equiv a \mod m$
$b_3)$ $a \equiv c \mod m$

Anmerkung

Die Eigenschaften in Teil b) des Satzes heißen Reflexivität, Symmetrie und Transitivität, d.h. die Relation *kongruent modulo* m ist eine Äquivalenzrelation auf $\mathbb{Z}$.

Mündlich: $b_1)$ und $b_2)$ werden mündlich begründet.

Wir beweisen nun $a_3)$. Die weiteren Behauptungen des Satzes könnt Ihr in der nächsten Aufgabe selber beweisen.

Tafelanschrieb

Beweis von $a_3)$: Wir wissen $a = b + km$, $c = d + lm$ mit $k, l \in \mathbb{Z}$.
Wir suchen ein $j \in \mathbb{Z}$, so dass $ac = bd + jm$.

$$\begin{aligned} ac &= (b+km)(d+lm) \\ &= bd + blm + kmd + kmlm \\ &= bd + \underbrace{(bl + kd + klm)}_{\in\mathbb{Z}} m \\ \Rightarrow \quad ac &= bd + jm \\ \Rightarrow \quad ac &\equiv bd \mod m \end{aligned}$$

□

Weiter auf nächster Seite

Aufgabe 3.6 (*Arbeitsblatt 3.3 (Rechenregeln für Kongruenzen), Aufgabe 4*)

Beweise die folgenden Aussagen:

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann $a + c \equiv b + d \mod m$.

b) Wenn $a \equiv b \mod m$, dann $-a \equiv -b \mod m$.

c) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann $a \equiv c \mod m$.

Hinweise: Zum Beweis von Teil a) kannst Du den Beweis von a_3), der an der Tafel steht, entsprechend anpassen.
Zum Beweis einer Kongruenz $a \equiv b \mod m$ genügt es, eine der folgenden drei äquivalenten Bedingungen nachzuweisen.

(1) $a - b$ ist durch m teilbar bzw. $a - b = km$ für ein $k \in \mathbb{Z}$
(2) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$
(3) a und b lassen beim Teilen durch m den selben Rest.

Datei: `Kryptographie34-Kongruenz-Rechenregeln`

Lösung: **a)** $a \equiv b \mod m$ und $c \equiv d \mod m$
$\Leftrightarrow \; a = b + km,\ c = d + lm$ mit geeigneten $k, l \in \mathbb{Z}$
$\Rightarrow \; a + c = b + d + km + lm = b + d + \underbrace{(k + l)}_{=k' \in \mathbb{Z}} m$
$\Rightarrow \; a + c \equiv b + d \mod m$

b) $a \equiv b \mod m \;\Leftrightarrow\; a = b + km$ mit einem geeigneten $k \in \mathbb{Z}$
$\Leftrightarrow \; -a = -b + (-k)m$
$\Rightarrow \; -a \equiv -b \mod m$

Alternative Lösung: $-1 \equiv -1 \mod m$ und $a \equiv b \mod m \overset{\text{Satz } a_2)}{\Rightarrow} -a \equiv -b \mod m$

c) $a \equiv b \mod m \;\Rightarrow\; a, b$ lassen beim Teilen durch m denselben Rest
$b \equiv c \mod m \;\Rightarrow\; b, c$ lassen beim Teilen durch m denselben Rest.
$\Rightarrow\; a, c$ lassen beim Teilen durch m denselben Rest.
$\Rightarrow\; a \equiv c \mod m$

Alternative Lösung: $a \equiv b \mod m$ und $b \equiv c \mod m$
$\Leftrightarrow \; a = b + km,\ b = c + lm$ mit geeigneten $k, l \in \mathbb{Z}$
$\Rightarrow \; a = (c + lm) + km = c + (k + l)m$ mit $k + l \in \mathbb{Z}$
$\Rightarrow \; a \equiv c \mod m$

Vorgehen: Ausgewählte Schüler:innen stellen ihre Lösung am Visualizer vor.

4.5 Die Quersummenregel

Tafelanschrieb

Satz (Quersummenregel): Wir schreiben $Q(a)$ für die Quersumme einer natürlichen Zahl a. Wir bilden so lange die Quersummen $Q(a),\ Q(Q(a)), \ldots$, bis sich eine Zahl b zwischen 1 und 9 ergibt. Dann gilt $a \equiv b \mod 9$.
Wenn $b = 9$, dann ist a durch 9 teilbar.

Beispiel: $a = 123456$: $Q(a) = 21,\ Q(Q(a)) = 3 \;\Rightarrow\; 123456 \equiv 3 \mod 9$

Mündlich: Das bedeutet, dass a zwar nicht durch 9, aber durch 3 teilbar ist.

Tafelanschrieb

Beweis 1) $a \equiv Q(a) \mod 9$:

Eine natürliche Zahl a mit $n+1$ Stellen können wir darstellen als

$$a = \boxed{a_n}\boxed{a_{n-1}} \ldots \boxed{\begin{array}{c}a_2\\ \mathsf{H}\end{array}}\boxed{\begin{array}{c}a_1\\ \mathsf{Z}\end{array}}\boxed{\begin{array}{c}a_0\\ \mathsf{E}\end{array}} \Rightarrow a = \underbrace{a_0 \cdot 1}_{\equiv a_0} + \underbrace{a_1 \cdot 10}_{\equiv a_1} + \underbrace{a_2 \cdot 100}_{\equiv a_2} + \ldots + \underbrace{a_n \cdot 10^n}_{\equiv a_n \bmod 9}.$$

$$\begin{array}{rcl} 10 & \equiv & 1 \bmod 9 \\ \overset{\text{Satz a}_4)}{\Rightarrow}\ 10^2 & \equiv & 1^2 \bmod 9 \\ \vdots & & \\ 10^n & \equiv & 1 \bmod 9 \end{array} \quad \overset{\text{Satz a}_3)}{\Rightarrow} \quad \begin{array}{rcl} a_1 \cdot 10 & \equiv & a_1 \cdot 1 \bmod 9 \\ a_2 \cdot 10^2 & \equiv & a_2 \cdot 1 \bmod 9 \\ \vdots & & \\ a_n \cdot 10^n & \equiv & a_n \cdot 1 \bmod 9 \end{array}$$

$$\overset{\text{Satz a}_2)}{\Rightarrow} \quad a \equiv \underbrace{a_0 + a_1 + a_2 + \ldots + a_n}_{=Q(a)} \mod 9.$$

2) $a \equiv Q(a)$, $Q(a) \equiv Q(Q(a)) \overset{\text{Satz b}_3)}{\Rightarrow} a \equiv Q(Q(a)) \Rightarrow a \equiv Q(Q(Q(a)))\ldots$ □

Anmerkung

Die Kraft der Quersummenregel zeigt sich daran, dass wir nun ganz leicht Umkehraufgaben lösen können.

Aufgabe 3.7 (*Arbeitsblatt 3.4 (Die Quersummenregel), Aufgabe 5*)

Gib zwei verschiedene 10-stellige Zahlen an, deren Ziffern nur aus Achten und Nullen bestehen, und die beim Teilen durch 9 den Rest 3 ergeben.

Datei: `Kryptographie37-Quersumme3Rueckwaerts`

Lösung: Z.B. $a = 8\,888\,880\,000$, $b = 8\,800\,880\,088$.

Weiter auf nächster Seite

4.6 Schriftliche Aufgaben (ohne Lösungen)

Aufgabe 3.8 (*Arbeitsblatt 3.5 (Schriftliche Aufgaben), Aufgabe 6*)

Wahr oder falsch? Kreuze an!

	wahr	falsch
Die Gleichung $2x \equiv 10 \mod 3$ besitzt mindestens eine Lösung $x \in \mathbb{Z}$.		
Die Gleichung $2x \equiv 10 \mod 3$ besitzt unendlich viele Lösungen $x \in \mathbb{Z}$.		
Die Gleichung $2x \equiv 7 \mod 4$ besitzt mindestens eine Lösung $x \in \mathbb{Z}$.		
Die Gleichung $2x \equiv 7 \mod 4$ besitzt unendlich viele Lösungen $x \in \mathbb{Z}$.		
Aus $x \equiv 3 \mod 5$ und $y \equiv 6 \mod 5$ folgt $xy \equiv 30 \mod 5$.		
Aus $x \equiv 5 \mod 3$ folgt $2x \equiv 10 \mod 6$.		
Aus $x \equiv 5 \mod 3$ folgt $2x \equiv 5 \mod 6$.		
Aus $x \equiv 5 \mod 3$ folgt $2x \equiv 10 \mod 3$.		
Für jede natürliche Zahl x gilt $x \equiv 0 \mod x$.		
Für jede natürliche Zahl x gilt $2x \equiv -x \mod x$.		

Datei: `Kryptographie390-Wahr-Falsch`

Aufgabe 3.9 (*Arbeitsblatt 3.5 (Schriftliche Aufgaben), Aufgabe 7*)

Gib die Menge L aller Lösungen der Kongruenzgleichung $3 \cdot x \equiv 1 \mod 11$ an.

$L =$ ☐.

Datei: `Kryptographie391-Kongruenzgleichung`

Aufgabe 3.10 (*Arbeitsblatt 3.5 (Schriftliche Aufgaben), Aufgabe 8*)

Mit $Q(x)$ wird die Quersumme der Zahl x bezeichnet. Gegeben ist die Zahl $a = 999\,888\,772$.

a) Berechne die angegebenen Quersummen.

$Q(a) =$ ☐, $Q(Q(a)) =$ ☐, $Q(Q(Q(a))) =$ ☐.

b) Gib jeweils eine möglichst kleine natürliche Zahl an, so dass die angegebene Kongruenz gilt.

$a \equiv$ ☐ $\mod 9$, $a \equiv$ ☐ $\mod 3$.

Datei: `Kryptographie392-Quersummenregel`

Aufgabe 3.11 (*Arbeitsblatt 3.5 (Schriftliche Aufgaben), Aufgabe 9*)

In dieser Aufgabe kannst Du alle Lösungen der Kongruenzgleichung

$$37 \cdot x \equiv 1 \mod 7 \qquad (*)$$

systematisch bestimmen.

a) Zunächst sollst Du die Kongruenzgleichung umformen. Das Äquivalenzzeichen bedeutet hier, dass sich die Lösungsmenge nicht ändert. Fülle die Kästchen aus.

$37 \cdot x \equiv 1 \mod 7$

$\Leftrightarrow$ Es gibt ein $k \in \mathbb{Z}$, so dass $37 \cdot x = 1 +$ ☐

$\Leftrightarrow$ Es gibt ein $k \in \mathbb{Z}$, so dass ☐ $\cdot x -$ ☐ $\cdot k = 1$

b) Bestimme mit dem erweiterten euklidischen Algorithmus eine Lösung der diophantischen Gleichung $37x + 7y = 1$.

Schritt 1:

Schritt 2:

$\mathrm{ggT}(37, 7) =$ ☐

Eine Lösung der Gleichung $37x + 7y = 1$: $(x \mid y) =$ ☐.

c) Gib alle Lösungen der diophantischen Gleichung $37x + 7y = 1$ an.

$(x \mid y) =$ ☐ mit $l \in \mathbb{Z}$.

d) Gib alle Lösungen der diophantischen Gleichung $37x - 7k = 1$ an.

$(x \mid y) =$ ☐ mit $l \in \mathbb{Z}$.

e) Gib die Lösungsmenge der Gleichung $(*)$ an.

$L =$ ☐.

Datei: `Kryptographie393-DiophantischeGleichung`

4.7 Ergänzung: Die Neunerprobe zur Kontrolle von Rechnungen:

$$\left.\begin{array}{rcl} a & \equiv & Q(a) \\ b & \equiv & Q(b) \end{array}\right\} \Rightarrow\ ab \equiv Q(ab) \text{ und } a+b \equiv Q(a+b)$$

Frage: $12345 \cdot 54321 \stackrel{?}{=} 671592745$
Neunerprobe: $12345 \equiv 6 \mod 9 \wedge 54321 \equiv 6 \mod 9 \Rightarrow 12345 \cdot 54321 \equiv 36 \equiv 9 \mod 9$
Aber $671592745 \equiv 46 \equiv 10 \equiv 1 \mod 9$

Also ist das Ergebnis falsch.

Aufgabe 3.12 (*Arbeitsblatt 3.4 (Die Neunerprobe), Zusatzaufgabe 3*)

Welche der folgenden Gleichungen sind garantiert falsch? (Ohne Taschenrechner!)

a) $12345 \cdot 54321 \stackrel{?}{=} 670592745$,

b) $6613598 \cdot 55500710 \stackrel{?}{=} 367359384654580$,

c) $6613598 \cdot 55500710 \stackrel{?}{=} 367059384654580$,

d) $6613598 \cdot 55500710 \cdot 432 \stackrel{?}{=} 158569654170778570$,

e) $123456709 + 6789402 + 878787487 + 1232123 \stackrel{?}{=} 1010365721$,

f) $123456709 + 6789402 + 878787487 + 1232123 \stackrel{?}{=} 1010265721$.

Datei: `Kryptographie38-Neunerprobe-zur-Kontrolle`

Lösung: **a)** $\underbrace{12345}_{\equiv 6 \mod 9} \cdot \underbrace{54321}_{\equiv 6 \mod 9} \stackrel{?}{=} \underbrace{670592745}_{\equiv 9 \mod 9} \Rightarrow$ könnte richtig sein (ist richtig),

b) $\underbrace{6613598}_{\equiv 2 \mod 9} \cdot \underbrace{55500710}_{\equiv 5 \mod 9} \stackrel{?}{=} \underbrace{367359384654580}_{\equiv 4 \mod 9} \Rightarrow$ falsch,

c) $\underbrace{6613598}_{\equiv 2 \mod 9} \cdot \underbrace{55500710}_{\equiv 5 \mod 9} \stackrel{?}{=} \underbrace{367059384654580}_{\equiv 1 \mod 9} \Rightarrow$ könnte richtig sein (ist richtig),

d) $\underbrace{6613598}_{\equiv 2 \mod 9} \cdot \underbrace{55500710}_{\equiv 5 \mod 9} \cdot \underbrace{432}_{\equiv 0 \mod 9} \stackrel{?}{=} \underbrace{158569654170778570}_{\equiv 1 \mod 9} \Rightarrow$ falsch,

e) $\underbrace{123456709}_{\equiv 1 \mod 9} + \underbrace{6789402}_{\equiv 0 \mod 9} + \underbrace{878787487}_{\equiv 1 \mod 9} + \underbrace{1232123}_{\equiv 5 \mod 9} \stackrel{?}{=} \underbrace{1010365721}_{\equiv 8 \mod 9} \Rightarrow$ falsch,

f) $\underbrace{123456709}_{\equiv 1 \mod 9} + \underbrace{6789402}_{\equiv 0 \mod 9} + \underbrace{878787487}_{\equiv 1 \mod 9} + \underbrace{1232123}_{\equiv 5 \mod 9} \stackrel{?}{=} \underbrace{1010265721}_{\equiv 7 \mod 9} \Rightarrow$ könnte richtig sein (ist richtig).

4.8 Weitere Aufgaben und Ergänzungen

Aufgabe 3.13 (*Arbeitsblatt 3.6 (Zusatzaufgaben), Zusatzaufgabe 4*)

Gegeben ist folgende Behauptung für $n \in \mathbb{Z}$:

$$\text{Entweder gilt } n^4 \equiv 1 \mod 5 \text{ oder } n^4 \equiv 0 \mod 5. \qquad (*)$$

a) Rechne nach, dass die Behauptung $(*)$ für $n = 1, 2, 3, 4, 5$ wahr ist.

b) Beweise mit den Rechenregeln für Kongruenzen: $a \equiv b \mod m \Rightarrow a^4 \equiv b^4 \mod m$.

c) Beweise, dass die Behauptung $(*)$ für alle $n \in \mathbb{Z}$ gilt.

Hinweis: Betrachte als erstes den Fall, dass $n = 5k + 1$ mit einem geeigneten $k \in \mathbb{Z}$ gilt. Welche Fälle müssen noch untersucht werden?

Datei: `Kryptographie35-KongruenzNhoch4`

Lösung: **a)** $1^4 = 1 \equiv 1 \mod 5$, $2^4 = 16 = 15 + 1 \equiv 1 \mod 5$, $3^4 = 81 = 80 + 1 \equiv 1 \mod 5$, $4^4 = 256 = 255 + 1 \equiv 1 \mod 5$, $5^4 = 625 \equiv 0 \mod 5$.

In allen Fällen ist $(*)$ wahr.

b) $a \equiv b \mod m \overset{\text{Satz a}_4)}{\Rightarrow} a^2 \equiv b^2 \mod m \overset{\text{Satz a}_4)}{\Rightarrow} a^4 = (a^2)^2 \equiv (b^2)^2 = b^4 \mod m$.

c) Fall 1: $n = 5k + 1$ mit einem geeigneten $k \in \mathbb{N} \Rightarrow n \equiv 1 \Rightarrow n^4 \equiv 1^4 = 1 \mod 5$.

Fall 2: $n = 5k + 2$ mit einem geeigneten $k \in \mathbb{N} \Rightarrow n \equiv 2 \Rightarrow n^4 \equiv 2^4 = 16 \equiv 1 \mod 5$.

Fall 3: $n = 5k + 3$ mit einem geeigneten $k \in \mathbb{N} \Rightarrow n \equiv 3 \Rightarrow n^4 \equiv 3^4 = 81 \equiv 1 \mod 5$.

Fall 4: $n = 5k + 4$ mit einem geeigneten $k \in \mathbb{N} \Rightarrow n \equiv 4 \Rightarrow n^4 \equiv 4^4 = 256 \equiv 1 \mod 5$.

Fall 5: $n = 5k + 5$ mit einem geeigneten $k \in \mathbb{N} \Rightarrow n \equiv 5 \Rightarrow n^4 \equiv 5^4 = 625 \equiv 0 \mod 5$.

Ideen für Aufgaben:

- Umkehraufgabe: Bestimme alle Zahlen x, für die $x \equiv 2 \mod 5$ gilt.
- Welche Zahl $x \in \mathbb{N}$ erfüllt die Gleichung $2x = 10$? Welche Zahlen erfüllen die Gleichung $2x \equiv 10 \mod 7$?
- Bestimme alle Lösungen der Gleichung $28x \equiv 12 \mod 20$.
- Zeige, dass $n^2 \equiv 0 \mod 4$ für alle geraden Zahlen $n \in \mathbb{N}$ und $n^2 \equiv 1 \mod 4$ für alle ungeraden $n \in \mathbb{N}$ gilt.
- Warum kann keine natürliche Zahl m mit $m \equiv 3 \mod 4$ als Summe von zwei Quadratzahlen geschrieben werden?

5 Unterrichtseinheit 4: Der Zahlenring

5.1 Vorbemerkungen

Ziele: Restklassen und Addition, Multiplikation von Restklassen. Satz vom Dividieren: Ist p eine Primzahl, dann kann in $\mathbb{Z}_p$ durch jede Restklasse außer $[0]$ dividiert werden.

Die Wiederholung wird am Beispiel der Uhr durchgeführt.

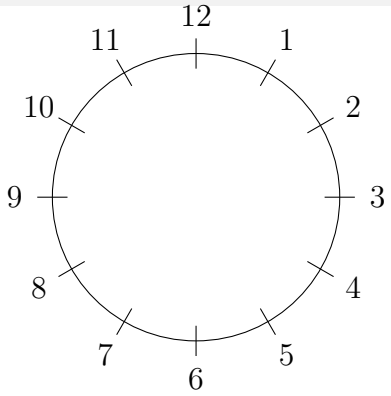
Die Kongruenz modulo 5 zieht sich als Beispiel durch die ganze Doppelstunde.

Die ganze Doppelstunde ist eher im Vorlesungsstil mit wenig Übungen.

5.2 Einführung

Vorgehen: Schüler:innen schreiben die ersten zwei Tafelanschribe nicht mit. Am Besten wird die Uhr bereits vor dem Beginn an die Tafel geschrieben oder am Visualizer gezeigt.

Tafelanschrieb



Auf der Uhr: 4 Uhr + 5 Stunden $=$ 9 Uhr
9 Uhr + 5 Stunden $=$ 2 Uhr

Auf der Uhr gilt 14 Uhr = 2 Uhr.

Mündlich: Was hat dies mit unserem Thema zu tun? (Kongruenz modulo 12)

Tafelanschrieb

Mathematisch: $14 \equiv 2 \mod 12$, denn

14 und 2 lassen beim Teilen durch 12 den selben Rest
$12 \mid (14 - 2)$
$14 = 1 \cdot 12 + 2$

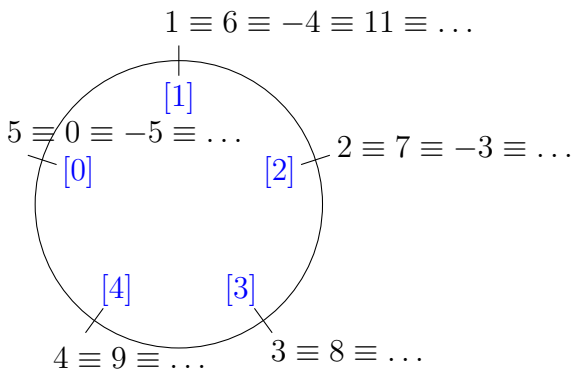
Mündlich: Weitere Anwendungen von Kongruenz im Alltag? (Minuten modulo 60, Wochentage modulo 7, Tagesdatum modulo 365)

> **Anmerkung**
> Es ist geschickt, die Eigenschaft mit dem selben Rest als Erste zu notieren. Dann kann man gut beim Namen *Rest*klasse darauf Bezug nehmen.

Tafelanschrieb

6. Rechnen mit Restklassen

Der Zahlenring modulo 5:



Vorgehen: Die blauen Restklassenbezeichnungen werden erst nach der Definition des Restklassenrings dazugeschrieben.

5.3 Restklassen

Tafelanschrieb

Betrachte alle Zahlen, die beim Teilen durch eine Zahl $m \in \mathbb{N}_+$ den selben Rest lassen. Diese Zahlen werden zu einer Menge zusammengefasst, der Restklasse.

Mündlich: Vom letzten Mal wissen wir: Genau dann, wenn zwei Zahlen beim Teilen durch m denselben Rest lassen, sind sie kongruent modulo m.

Tafelanschrieb

Definition: Die Restklasse $[a]$ von a modulo m ist definiert durch

$$[a] := \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

a heißt Repräsentant der Restklasse $[a]$.

Mündlich: Mengenschreibweise verbalisieren.

Tafelanschrieb

Beispiele modulo 5:

$$\begin{array}{llllllll} [0] & = & \{\ldots,-10,-5,0,5,10,\ldots\} & = & [5] & = & \ldots & \\ [1] & = & \{\ldots,-9,-4,1,6,11,\ldots\} & = & [6] & = & [-4] & = \ldots \\ [2] & = & \ldots & & & & & \\ [3] & = & \ldots & = & [8] & = & \ldots & \\ [4] & = & \ldots & & & & & \end{array}$$

0 und 5 sind verschiedene Repräsentanten von $[0]$.

Mündlich: Gibt es noch weitere Restklassen modulo 5?

Vorgehen: Wenn die Schüler:innen Restklassen wie z.B. $[6]$ nennen, werden diese an die enstprechende Restklasse dazugeschrieben. Wenn die Schüler:innen erkennen, dass es keine weiteren gibt, werden noch drei ergänzt, wie oben bereits geschehen.

Mündlich: Durch die Restklassenbildung wird aus Kongruenz Gleichheit: $1 \equiv 6 \mod 5$ bedeutet dasselbe wie $[1] = [6]$ in $\mathbb{Z}_5$.

Anmerkung
Man sollte nicht überrascht sein, wenn von Schüler:innen behauptet wird, dass z.B. 2883 ein Element von $[3]$ ist.

Anmerkung
Sprechweise: „Die Restklasse $[a]$“ oder „Die Restklasse von a“.

Tafelanschrieb
Definition: Die Menge aller Restklassen modulo m heißt Restklassenring modulo m, schreibe $\mathbb{Z}_m$.

Beispiel: $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$.

Vorgehen: Nun werden die Restklassen farbig in den Zahlenring modulo 5 eingetragen.

Aufgabe 4.1 (*Arbeitsblatt 4.1 (Restklassen), Aufgabe 1*)

a) Gib die Elemente der Restklasse $[3]$ modulo 7 an.

$[3] =$ $\{\ldots, -11, -4, 3, 10, 17, \ldots\}$. oder $\{3 + 7k : k \in \mathbb{Z}\}$

b) Gegeben sind die Restklassen $[49]$, $[16]$ und $[-10]$ modulo 7. Gib jeweils eine möglichst kleine nichtnegative ganze Zahl x an, so dass $[49] = [x]$ bzw. $[16] = [x]$ bzw. $[-10] = [x]$ gilt.

$[49] =$ $[0]$, $[16] =$ $[2]$, $[-10] =$ $[4]$.

c) Gib alle Elemente von $\mathbb{Z}_7$ an.

$\mathbb{Z}_7 =$ $\{[0], [1], [2], [3], [4], [5], [6]\}$.

Datei: `Kryptographie40-Z7-Elemente`

Lösung: Ist bereits im Aufgabentext enthalten.

5.4 Rechnen mit Restklassen

Mündlich: Wir wollen mit Restklassen rechnen können. Dazu definieren wir nun Addition und Multiplikation von Restklassen.

Tafelanschrieb
Definition: Für $a, b \in \mathbb{Z}$ definiert man

$$\begin{aligned} [a] + [b] &:= [a + b] \\ [a] \cdot [b] &:= [ab] \end{aligned}$$

Mündlich: Man definiert hier eine Addition von Mengen. Das ist eine neue Addition. Weil sie durch die bekannte Addition von ganzen Zahlen definiert wird, verwendet man das selbe Symbol.

Tafelanschrieb

Beispiele modulo 5:

$$\begin{aligned} [2]+[2] &= [4] \\ [3]+[4] &= [7] = [2] \\ [3]\cdot[4] &= [12] = [2] \\ [-2]\cdot[-1] &= [2] \\ [8]\cdot[9] &= [72] = [2] \end{aligned}$$

Mündlich: Wir einigen uns darauf, dass die Ergebnisse beim Rechnen modulo 5 immer als Restklassen von Zahlen zwischen 0 und 4 dargestellt werden. Dann können die Ergebnisse besser verglichen werden. Außerdem kann man mit kleineren Zahlen besser weiterrechnen.

Mündlich: Wir sehen: $[3] = [-2] = [8]$ und $[4] = [-1] = [9]$, und alle drei Produkte $[3]\cdot[4]$, $[-2]\cdot[-1]$, $[8]\cdot[9]$ ergeben dieselbe Restklasse. Wir klären nun, dass das immer so ist. Erst dann ist die Definition der Multiplikation sinnvoll.

Tafelanschrieb

Satz: Ist $[a] = [a']$ und $[b] = [b']$, so gilt $[a\cdot b] = [a'\cdot b']$ und $[a+b] = [a'+b']$.

Beweis: Ist $[a] = [a']$ und $[b] = [b']$, so folgt:

$$\begin{aligned} & a \equiv a' \mod m \quad \text{und} \quad b \equiv b' \mod m \\ \overset{\text{Rechenregeln für Kongruenzen}}{\Rightarrow} \quad & ab \equiv a'b' \mod m \quad \text{und} \quad a+b \equiv a'+b' \mod m \\ \Rightarrow \quad & [ab] = [a'b'] \quad \text{und} \quad [a+b] = [a'+b'] \end{aligned}$$

□

Mündlich: Es ist egal, welche Repräsentanten der Restklassen $[a]$ und $[b]$ für die Berechnung von $[a]\cdot[b]$ verwendet werden, als Ergebnis kommt immer die selbe Restklasse heraus.

Aufgabe 4.2 (*Arbeitsblatt 4.2 (Rechnen mit Restklassen), Aufgabe 2*)

Fülle die Verknüpfungstabelle für die Addition und Multiplikation in $\mathbb{Z}_5$ aus. Achtung: Es dürfen nur die Bezeichnungen $[0], \ldots, [4]$ verwendet werden, also anstelle von $[8]$ muss $[3]$ geschrieben werden.

Datei: `Kryptographie41-VerknuepfungstabellenZ5`

Lösung:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Anmerkung

Die folgende Zusatzaufgabe zeigt, dass Potenzen in Restklassenringen unerwartete Ergebnisse liefern können.

Aufgabe 4.3 (*Arbeitsblatt 4.2 (Rechnen mit Restklassen), Zusatzaufgabe 1*)

Bestimme alle natürlichen Potenzen, d.h. $[a]^1$, $[a]^2$, $[a]^3$, $[a]^4$, ...

a) von $[4]$ in $\mathbb{Z}_5$, **b)** von $[3]$ in $\mathbb{Z}_{11}$, **c)** jeweils von $[2], [3], [5]$ in $\mathbb{Z}_6$.

Datei: `Kryptographie44-Potenzen`

Lösung: **a)** $[4]^2 = [1],\ [4]^3 = [4],\ [4]^4 = [1],$

$$\text{also } [4]^n = \begin{cases} [4], & n \text{ ungerade} \\ [1], & n \text{ gerade} \end{cases}$$

b) $[3]^2 = [9],\ [3]^3 = [5],\ [3]^4 = [4],\ [3]^5 = [1],\ [3]^6 = [3],$

$$\text{also } [3]^n = \begin{cases} [3] & \text{falls } n \equiv 1 \mod 5 \\ [9] & \text{falls } n \equiv 2 \mod 5 \\ [5] & \text{falls } n \equiv 3 \mod 5 \\ [4] & \text{falls } n \equiv 4 \mod 5 \\ [1] & \text{falls } n \equiv 0 \mod 5 \end{cases}$$

c) $[2]^2 = [4],\ [2]^3 = [2],\ [2]^4 = [4],\ [2]^5 = [2],$

$$\text{also } [2]^n = \begin{cases} [4], & n \text{ gerade} \\ [2], & n \text{ ungerade} \end{cases}$$

$[3]^2 = [3],\ [3]^3 = [3]$, also $[3]^n = [3]$ für alle n.

$[5]^2 = [1],\ [5]^3 = [5],\ [5]^4 = [1],$

$$\text{also } [5]^n = \begin{cases} [5], & n \text{ ungerade} \\ [1], & n \text{ gerade} \end{cases}$$

Mündlich: Nun können wir überlegen, wie es mit Differenzen und Quotienten in $\mathbb{Z}_5$ aussieht.

Vorgehen: Schüler:innen schreiben die nächsten beiden Tafelanschriebe nicht mit.

Für die Überlegungen sollten die ausgefüllten Tabellen für Addition und Multiplikation in $\mathbb{Z}_5$ präsentiert werden.

Den Schüler:innen etwas Zeit zum Nachdenken geben.

Tafelanschrieb

In $\mathbb{Z}_5$: $[1] - [2] =$

$[1] - [4] =$

$\dfrac{[1]}{[2]} =$

$\dfrac{[2]}{[3]} =$

Tafelanschrieb

Aus der Additionstabelle für $\mathbb{Z}_5$: $[4] + [2] = [1]$

$$\Rightarrow \begin{cases} [1] - [2] = [4] = [-1] \\ [1] - [4] = [2] = [-3] \end{cases}$$

Vorgehen: Ab jetzt schreiben Schüler:innen wieder mit.

Tafelanschrieb

Satz: für $a, b \in \mathbb{Z}$ gilt $[a] - [b] = [a - b]$.

Beweis: $[a - b] + [b] = [a - b + b] = [a] \ \Rightarrow\ [a - b] = [a] - [b]$.

Anmerkung
Wie die Subtraktion funktioniert, ist für Schüler:innen offensichtlich. Bei der Division gibt es Schwierigkeiten. Unsere Schüler:innen hatten die Idee, im Zähler so oft $m = 5$ zu addieren, bis die Vertreter der Restklassen teilbar sind:

$$\frac{[1]}{[2]} = \frac{[6]}{[2]} = [3].$$

Diese Idee ist richtig und funktioniert gut, so lange der Bruch definiert ist, vgl. Aufgabe 4.5. Im allgemeinen Fall führt diese Idee auf die selbe diophantische Gleichung wie die im Beweis des Satzes über die Existenz von Brüchen, der später in dieser Stunde geführt wird. Aber die Methode hier verwendet nicht die Definition eines Bruches. Ein Bruch ist definiert als die Zahl, die mit dem Nenner multipliziert den Zähler ergibt. Brüche werden über die Multiplikation definiert! Deshalb ist es gut, bei der folgenden Berechnung auf die Multiplikationstabelle hinzuweisen.

Tafelanschrieb

Beispiel zur Division: Was ist $\frac{[1]}{[2]}$ in $\mathbb{Z}_5$?

$\frac{[1]}{[2]} = [x] \Leftrightarrow [2] \cdot [x] = [1]$

Multiplikationstabelle in $\mathbb{Z}_5 \Rightarrow [x] = [3]$

Genauso: $\frac{[2]}{[3]} = [4]$, da $[3] \cdot [4] = [2]$.

Vorgehen: Nun kann in der Multiplikationstabelle an Hand von Pfeilen visualisiert werden, wie man den Wert der beiden Brüche findet.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

$[3] = \frac{[1]}{[2]}$

Mündlich: Man startet links beim Nenner, geht in der Zeile nach rechts bis zum Zähler, dann steht in der selben Spalte ganz oben die Restklasse des Bruches.

Anmerkung
Auf dem folgenden Arbeitsblatt sind eine Additionstabelle für $\mathbb{Z}_9$ und eine Multiplikationstabelle für $\mathbb{Z}_{11}$ angegeben.

Aufgabe 4.4 (*Arbeitsblatt 4.3 (Differenzen und Quotienten von Restklassen), Aufgabe 3*)

a) Bestimme in $\mathbb{Z}_9$: $[1]-[8]=$ $\boxed{[2]}$ und $-[4]=$ $\boxed{[5]}$.

b) Bestimme in $\mathbb{Z}_{11}$ die Restklassen der angegebenen Brüche. Lies die Ergebnisse in der unten stehenden Multiplikationstabelle ab und begründe jeweils Dein Ergebnis.

b₁) $\frac{[1]}{[2]}=$ $\boxed{[6]}$, denn $[2]\cdot$ $\boxed{[6]}$ $=$ $\boxed{[1]}$.

b₂) $\frac{[1]}{[4]}=$ $\boxed{[3]}$, denn $\boxed{[4]\cdot[3]=[1]}$

b₃) $\frac{[2]}{[4]}=$ $\boxed{[6]}$, denn $\boxed{[4]\cdot[6]=[2]}$

Datei: `Kryptographie42-Inverse-Z9-Z11`

Lösung: Ist bereits im Aufgabentext enthalten.

Mündlich: Das sind erstaunliche Ergebnisse. $\frac{1}{2}=6$ hört sich doch verrückt an. Oder in der nächsten Aufgabe $\frac{1}{3}=3$.

Anmerkung
Wenn ein Bruch definiert ist, kann man getrost mit ganzen Zahlen kürzen, das sollte die Aufgabe auch zeigen:

$$\frac{[2]}{[4]}=\frac{[1]}{[2]}.$$

In $\mathbb{Z}_{11}$ kann man dann folgendermaßen rechnen

$$\frac{[1]}{[2]}=\frac{[1+11]}{[2]}=\frac{[12]}{[2]}=[6].$$

Anmerkung
Die folgende Aufgabe soll zur Frage hinführen, ob Brüche immer definiert sind.

Aufgabe 4.5 (*Arbeitsblatt 4.3 (Differenzen und Quotienten von Restklassen), Aufgabe 4*)

a) Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_4$ aus.

b) Versuche, in $\mathbb{Z}_4$ die Restklassen folgender Brüche zu bestimmen.

$\frac{[1]}{[3]}$ $\boxed{=[3]}$,

$\frac{[1]}{[2]}$ $\boxed{\text{gibt es nicht, denn es gibt keine Restklasse } [x] \text{ mit } [x]\cdot[2]=[1]}$,

$\frac{[2]}{[2]}$ $\boxed{\begin{array}{l}\text{Für } \frac{[2]}{[2]} \text{ gibt es zwei Möglichkeiten: } [1] \text{ oder } [3].\\ \text{Dieser Bruch kann also nicht definiert werden.}\end{array}}$.

Datei: `Kryptographie43-Z4`

Lösung: **a)**

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

b) Ist bereits im Aufgabentext enthalten.

> **Anmerkung**
> Dass $\frac{[1]}{[2]}$ in $\mathbb{Z}_4$ nicht definiert ist, sieht man auch dadurch, dass $1 + 4k$ nie durch 2 teilbar ist. Beim Bruch $\frac{[2]}{[2]}$ könnte man denken, dass $\frac{[2]}{[2]} = [1]$ gilt. Aber man sieht, dass auch $\frac{[2]}{[2]} = \frac{[6]}{[2]} = [3]$ gelten könnte. So zeigt auch die in der vorigen Anmerkung beschriebene Methode, dass der Bruch nicht definiert ist.

Mündlich: Wir haben gesehen, dass Brüche nicht immer definiert sind. Nun klären wir, wann Brüche definiert sind. Beachte, dass in $\mathbb{Z}_4$ manche Brüche nicht definiert sind, und dass 4 keine Primzahl ist.

Tafelanschrieb

Existenz von Brüchen in $\mathbb{Z}_m$: Sei $m \in \mathbb{N}_+$, $a \in \{0, 1, \ldots, m-1\}$ und $b \in \{1, 2, \ldots, m-1\}$.

Mündlich: Wir betrachten den Bruch $[a]$ durch $[b]$. Deshalb müssen wir voraussetzen, dass die Restklasse $[b]$ von der Restklasse $[0]$ verschieden ist.

Tafelanschrieb

$$\begin{aligned} \frac{[a]}{[b]} = [x] &\Leftrightarrow [a] = [b] \cdot [x] = [bx] \\ &\Leftrightarrow a \equiv bx \mod m \\ &\Leftrightarrow a - bx = km \quad \text{für ein } k \in \mathbb{Z} \\ &\Leftrightarrow a = b\underbrace{x}_{\text{gesucht}} + m\underbrace{k}_{\text{unbekannt}} \end{aligned}$$

Dies ist eine diophantische Gleichung für die Unbekannten $x, k \in \mathbb{Z}$.

Wir wissen: Falls $\text{ggT}(b, m) \mid a$, ist die Gleichung lösbar.

Sei nun m eine Primzahl. Dann gilt $\text{ggT}(b, m) = 1$.

Mündlich: Klären, warum der ggT gleich 1 ist.
Darauf hinweisen, dass es nun für jedes a Lösungen $(x \mid k)$ gibt.

Tafelanschrieb

$\Rightarrow$ Für jedes $a \in \mathbb{N}$ existiert eine Lösung $(x_0 \mid k_0)$. Alle Lösungen sind durch

$$(x \mid k) = (x_0 + lm \mid k - lb) \text{ mit } l \in \mathbb{Z}$$

gegeben. Wir suchen nur $x = x_0 + lm$ und sehen $[x] = [x_0]$. Also ist $[x]$ eindeutig.

Damit ist bewiesen:

Mündlich: Darauf hinweisen, dass nun p an Stelle von m geschrieben wird, damit sofort klar ist, dass hier eine Primzahl gemeint ist.

Tafelanschrieb

Satz vom Dividieren: Ist p eine Primzahl, und sind $a \in \{0, 1, \ldots, p-1\}$, $b \in \{1, \ldots, p-1\}$, so besitzt die Gleichung

$$[b] \cdot [x] \;=\; [a] \qquad \text{in } \mathbb{Z}_p$$

genau eine Lösung $[x]$, d.h. $\dfrac{[a]}{[b]} := [x]$ ist definiert.

Aufgabe 4.6 (*Arbeitsblatt 4.4 (Quotienten von Restklassen), Aufgabe 5*)

In $\mathbb{Z}_{37}$ soll der Bruch $\dfrac{[5]}{[33]}$ bestimmt werden.

a) Führe den euklidischen Algorithmus zur Bestimmung von $\mathrm{ggT}(37, 33)$ durch.

b) Erweitere den euklidischen Algorithmus, um eine Lösung $(k \mid l)$ der diophantischen Gleichung $k \cdot 33 + l \cdot 37 = 1$ zu berechnen.

c) Sei $(k \mid l)$ die in b) bestimmte Lösung. Bestimme mit dem k aus dieser Lösung die Restklasse $[x] = [k] \cdot [33]$ in $\mathbb{Z}_{37}$, wobei $0 \le x < 37$ gelten soll.

d) Bestimme die Restklasse $[y] = \dfrac{[1]}{[33]}$, wobei $0 \le y < 37$ gelten soll.

e) Bestimme die Restklasse $[z] = \dfrac{[5]}{[33]}$, wobei $0 \le z < 37$ gelten soll.

Datei: `Kryptographie45-Bruch-mit-Euklid`

Lösung: **a)** und **b)**:

$$\begin{array}{rcl|rcl} 37 &=& 1 \cdot 33 + 4 & 4 &=& 37 - 1 \cdot 33 \\ 33 &=& 8 \cdot 4 + 1 & 1 &=& 33 - 8 \cdot 4 \\ 4 &=& 4 \cdot 1 & &=& 33 - 8(37 - 1 \cdot 33) \;=\; 9 \cdot 33 + 8 \cdot 37 \end{array}$$

$\Rightarrow$ $(k \mid l) = (9 \mid 8)$ ist eine Lösung der Gleichung $k \cdot 33 + l \cdot 37 = 1$.

c) Nach b) gilt $9 \cdot 33 \equiv 1 \mod 37$ $\Rightarrow$ $[9 \cdot 33] = [1]$, also $[x] = [1]$.

d) Aus c) folgt $[y] = \dfrac{[1]}{[33]} = [9]$, denn $[9] \cdot [33] = [9 \cdot 33] = [1]$.

e) Aus d) folgt $[z] = [5] \cdot [9] = [45] = [45 - 37] = [8]$.

Probe: $[8] \cdot [33] = [264] = [264 - 7 \cdot 37] = [264 - 259] = [5]$. ✓

5.5 Schriftliche Aufgaben (ohne Lösungen)

Aufgabe 4.7 (*Arbeitsblatt 4.5 (Schriftliche Aufgaben), Aufgabe 6*)

Gib jeweils die Elemente der Restklasse an.

a) In $\mathbb{Z}_3$ gilt $[4] =$ $\square$.

b) In $\mathbb{Z}_8$ gilt $[4] =$ $\square$.

Datei: `Kryptographie490-RestklassenZ3-Z8`

Aufgabe 4.8 (*Arbeitsblatt 4.5 (Schriftliche Aufgaben), Aufgabe 7*)

Gib alle Elemente von $\mathbb{Z}_9$ an.

$\mathbb{Z}_9 =$ $\square$.

Datei: `Kryptographie491-ElementeZ9`

Aufgabe 4.9 (*Arbeitsblatt 4.5 (Schriftliche Aufgaben), Aufgabe 8*)

Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_7$ aus.

Achtung: Es dürfen nur die Bezeichnungen $[0], \ldots, [6]$ verwendet werden.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Datei: `Kryptographie492-MultiplikationstabelleZ7`

Aufgabe 4.10 (*Arbeitsblatt 4.5 (Schriftliche Aufgaben), Aufgabe 9*)

Gesucht sind die Restklassen der folgenden Brüche in $\mathbb{Z}_{13}$. Lies die Ergebnisse in der unten stehenden Multiplikationstabelle ab und begründe jeweils Dein Ergebnis.

a) $\frac{[1]}{[3]} = \square$, denn $[3]\cdot \square = \square$.

b) $\frac{[1]}{[4]} = \square$, denn $\square$

c) $\frac{[3]}{[5]} = \square$, denn $\square$

Multiplikationstabelle für $\mathbb{Z}_{13}$:

·	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[12]	[1]	[3]	[5]	[7]	[9]	[11]
[3]	[0]	[3]	[6]	[9]	[12]	[2]	[5]	[8]	[11]	[1]	[4]	[7]	[10]
[4]	[0]	[4]	[8]	[12]	[3]	[7]	[11]	[2]	[6]	[10]	[1]	[5]	[9]
[5]	[0]	[5]	[10]	[2]	[7]	[12]	[4]	[9]	[1]	[6]	[11]	[3]	[8]
[6]	[0]	[6]	[12]	[5]	[11]	[4]	[10]	[3]	[9]	[2]	[8]	[1]	[7]
[7]	[0]	[7]	[1]	[8]	[2]	[9]	[3]	[10]	[4]	[11]	[5]	[12]	[6]
[8]	[0]	[8]	[3]	[11]	[6]	[1]	[9]	[4]	[12]	[7]	[2]	[10]	[5]
[9]	[0]	[9]	[5]	[1]	[10]	[6]	[2]	[11]	[7]	[3]	[12]	[8]	[4]
[10]	[0]	[10]	[7]	[4]	[1]	[11]	[8]	[5]	[2]	[12]	[9]	[6]	[3]
[11]	[0]	[11]	[9]	[7]	[5]	[3]	[1]	[12]	[10]	[8]	[6]	[4]	[2]
[12]	[0]	[12]	[11]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Datei: `Kryptographie493-Brueche-Z13`

Weiter auf nächster Seite

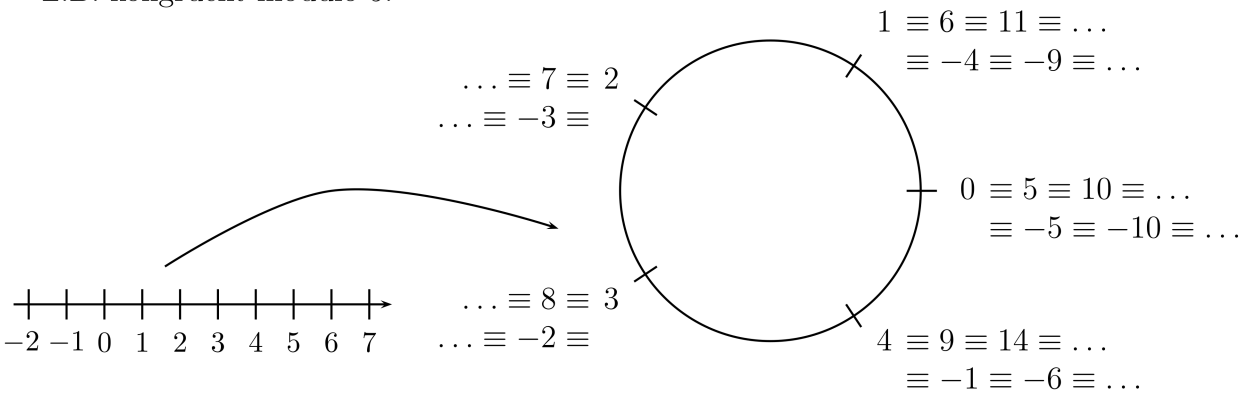
5.6 Ergänzungen

Alternativer Einstieg über das Zusammenrollen des Zahlenstrahls (2016):

Wiederholung: $a \equiv b \mod m$ falls $a - b$ durch m teilbar ist
bzw. falls $a = b + km$ für ein $k \in \mathbb{Z}$.

Die Beziehung kongruent rollt die Zahlengerade zu einem Zahlenring zusammen:

Z.B. kongruent modulo 5:



Zusammenfassen zu Mengen:

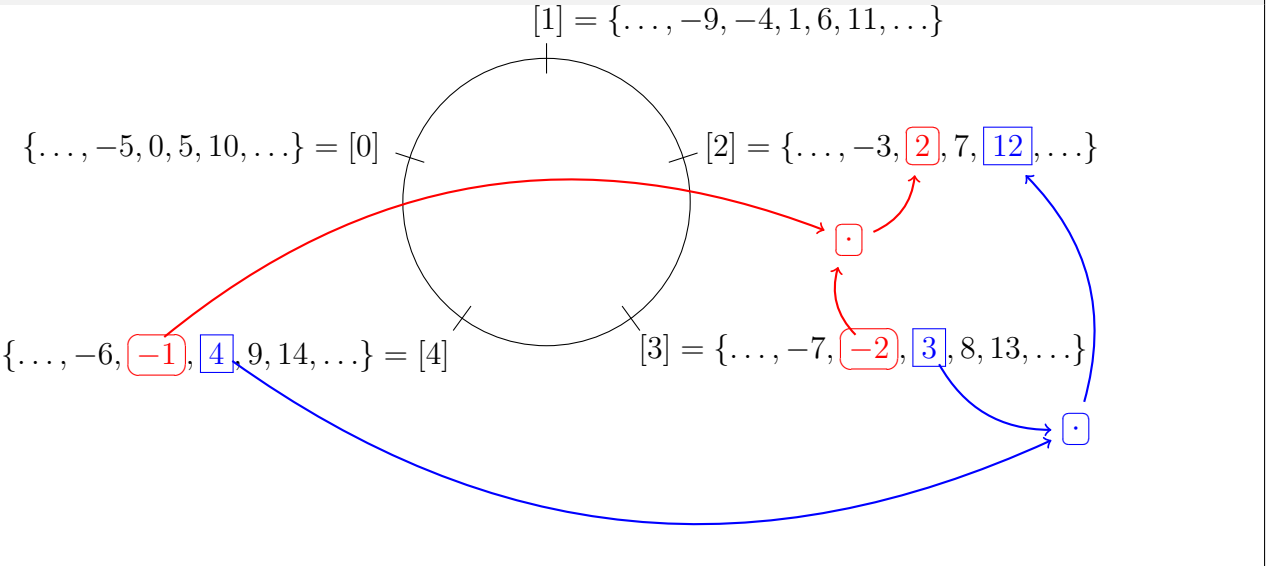
$$\begin{aligned} \{\ldots, -9, -4, 1, 6, 11, \ldots\} &= \{b \in \mathbb{Z} : b \equiv 1 \mod 5\} =: [1] \\ \{\ldots, -10, -5, 0, 5, 10, \ldots\} &= \{b \in \mathbb{Z} : b \equiv 0 \mod 5\} =: [0] \end{aligned}$$

Alle Elemente der Menge [1] ergeben beim Teilen durch 5 denselben Rest, deshalb nennt man eine solche Menge **Restklasse**.

> **Anmerkung**
> Man kann einen flexiblen Zahlenstrahl basteln und auf dem Visualizer zusammenrollen.

Visualisierung der Unabhängigkeit des Produkts vom Repräsentanten:

Multiplikation in $\mathbb{Z}_5$



Nicht-Existenz von Brüchen: An den Überlegungen zur Existenz von Brüchen kann man auch sehen, dass Brüche nur dann definiert sind, wenn $\mathrm{ggT}(b,m)=1$ gilt. Denn andernfalls, wenn eine Lösung x_0 existiert, sind alle Lösungen der diophantischen Gleichung gegeben durch

$$x = x_0 + l\,\frac{m}{\mathrm{ggT}(b,m)}\ (l\in\mathbb{Z}).$$

Offensichtlich sind dies Elemente mehrerer Restklassen modulo m:

$$\begin{aligned} x &= x_0 + sm \quad \text{mit } s\in\mathbb{Z} \\ x &= x_0 + \frac{m}{\mathrm{ggT}(b,m)} + sm \quad \text{mit } s\in\mathbb{Z} \quad (\text{setze } l = 1 + s\mathrm{ggT}(b,m)) \\ &\vdots \end{aligned}$$

D.h. die Gleichung $[a]=[b]\cdot[x]$ hat mindestens die zwei Lösungen

$$[x]=[x_0] \text{ und } [x]=\left[x_0+\frac{m}{\mathrm{ggT}(b,m)}\right]\neq[x_0].$$

Das bedeutet: Im Fall $\mathrm{ggT}(b,m)\neq 1$ gibt es entweder keine Lösung der Gleichung $[a]=[b]\cdot[x]$ oder mindestens zwei. Der Bruch $\dfrac{[a]}{[b]}$ ist in diesem Fall nicht definiert.

Satz vom Nullprodukt: Die Aussage „Aus $a\cdot b=0$ folgt $a=0$ oder $b=0$“ gilt in $\mathbb{Z}_p$ genau dann, wenn p eine Primzahl ist.

Beweis: Fall 1 „p ist eine Primzahl“: Sei $[a]\cdot[b]=[0]$.
Falls $[a]=[0]$ gilt, sind wir fertig.
Falls $[a]\neq[0]$, dann existiert der Bruch $\dfrac{[1]}{[a]}$ in $\mathbb{Z}_p$.

$$\Rightarrow\ [b]=\frac{[1]}{[a]}\cdot[a]\cdot[b]=\frac{[1]}{[a]}\cdot[0]=[0].$$

Also muss $[b]=[0]$ gelten.

Fall 2 „p ist keine Primzahl“: Dann gibt es zwei natürliche Zahlen m,n mit $p=m\cdot n$. Es folgt

$$[m]\neq[0]\ \wedge\ [n]\neq[0]\ \wedge\ [m]\cdot[n]=[mn]=[p]=[0].$$

Es gibt also mindestens die zwei Nullteiler $[m],[n]$.

Weiter auf nächster Seite

5.7 Weitere Aufgaben

> **Anmerkung**
> Die folgende Aufgabe besteht aus einem Teil von Zusatzaufgabe 1.

Aufgabe 4.11 (*Arbeitsblatt 4.6 (Zusatzaufgaben), Zusatzaufgabe 2*)

a) Bestimme in $\mathbb{Z}_5$ die angegebenen Potenzen von $[4]$.

$[4]^1 = \boxed{[4]}$, $[4]^2 = \boxed{[1]}$, $[4]^3 = \boxed{[4]}$, $[4]^4 = \boxed{[1]}$, $[4]^5 = \boxed{[4]}$.

b) Bestimme in $\mathbb{Z}_5$ die angegeben Potenzen von $[3]$.

$[3]^1 = \boxed{[3]}$, $[3]^2 = \boxed{[4]}$, $[3]^3 = \boxed{[2]}$, $[3]^4 = \boxed{[1]}$, $[3]^5 = \boxed{[3]}$.

c) Bestimme in $\mathbb{Z}_6$ die angegeben Potenzen von $[3]$.

$[3]^1 = \boxed{[3]}$, $[3]^2 = \boxed{[3]}$, $[3]^3 = \boxed{[3]}$, $[3]^4 = \boxed{[3]}$, $[3]^5 = \boxed{[3]}$.

Datei: `Kryptographie46-Potenzen`

Lösung: Ist bereits im Aufgabentext enthalten.

Aufgabe 4.12 (*Arbeitsblatt 4.6 (Zusatzaufgaben), Zusatzaufgabe 3*)

Bestimme in $\mathbb{Z}_{89}$ den Wert $\frac{[7]}{[20]}$ durch Lösung der Gleichung $20k + 89l = 7$.

Datei: `Kryptographie47-Bruch-in-Z89`

Lösung:

$$\begin{array}{rcl|rcl} 89 &=& 4\cdot 20+9 & 9 &=& 89-4\cdot 20 \\ 20 &=& 2\cdot 9+2 & 2 &=& 20-2\cdot 9 \\ 9 &=& 4\cdot 2+1 & 1 &=& 9-4\cdot 2 \\ 2 &=& 2\cdot 1 & &=& 9-4(20-2\cdot 9) \;=\; 9\cdot 9-4\cdot 20 \\ & & & &=& 9(89-4\cdot 20)-4\cdot 20 \;=\; 9\cdot 89-40\cdot 20 \\ & & & &\Rightarrow& 20\cdot(-40)+89\cdot 9 \;=\; 1 \end{array}$$

Da die rechte Seite $7 \cdot \text{ggT}(89, 20)$ ist, müssen die erhaltenen Zahlen noch mit 7 multipliziert werden $\Rightarrow\ (k, l) = (-280, 63)$

Mit $k = -280 \equiv 4 \cdot 89 - 280 = 76 \mod 89$ folgt $\frac{[7]}{[20]} = [76]$ in $\mathbb{Z}_{89}$

Probe: $[20] \cdot [76] = [1520] = [1520 - 890] = [630] = [630 - 7 \cdot 89] = [7]$ ✓

6 Unterrichtseinheit 5: Entschlüsselung geheimer Botschaften

6.1 Vorbemerkungen

In dieser Einheit lernen die Schüler:innen die klassischen Verfahren *Caesar*-, *Permutations*- und *Vigenère*-Verschlüsselung kennen. Einerseits macht es Spaß, mit den angegebenen Hilfsmitteln Texte zu entschlüsseln. Andererseits merken die Schüler:innen, dass diese Verfahren unsicher sind, auch wenn es etwas Mühe bereitet, einen permutationsverschlüsselten Text zu entschlüsseln.

Für die nächste Einheit ist es wichtig, dass die Schüler:innen die Vigenère-Verschlüsselung beherrschen, denn dort sollen sie mit Hilfe eines übermittelten Passwortes einen verschlüsselten Text von Hand entschlüsseln. Als Vorbereitung dazu sind die Caesar- und die Permutationsverschlüsselung sehr hilfreich.

Man kann die Caesar-Entschlüsselung gut mit den Alphabetstreifen veranschaulichen, die im Kapitel 15 zur Verfügung gestellt werden. Für die anderen Verfahren (und für Caesar) werden zwei Programme verwendet: Das Programm `CrypTool` und der Editor `Emacs` (ja, den gibt es immer noch).

Im Programm `CrypTool` gibt es sehr viele verschiedene Verschlüsselungsverfahren, und sie werden auch erklärt. Wir verwenden nur einen Bruchteil des Angebots. Leider hat dieses Programm (noch?) kein gutes Tool, um Substitutionsverschlüsselung zu knacken. Es gibt zwar eine Häufigkeits-Analyse, die wir auch verwenden, aber um den Text damit zu entschlüsseln, muss man im Text buchstabenweise ersetzen, und da ist der Entschlüsselungsmodus im Emacs ideal.

Vom Programm CrypTool gibt es verschiedene Varianten. Im Präsenz-Workshop haben wir uns für `JCrypTool` entschieden, denn dann wird keine Internet-Verbindung benötigt. Im Online-Workshop dagegen wurde `CrypTool-Online` verwendet, das läuft im Browser.

Im **Präsenz-Workshop** zeigt die Erfahrung, dass die originalen verschlüsselten Texte in einem Backup-Verzeichnis gespeichert werden müssen. Es passiert immer wieder, dass Schüler:innen die verschlüsselten Dateien ändern und abspeichern.

Die verschlüsselten Texte heißen `text1-Caesar.txt`, ..., `text6-Vigenere.txt` und sind in einem Unterverzeichnis `backup` gespeichert. Die Schüler:innen rufen nach dem Einloggen eine Batch-Datei auf. Das ist eine Datei, die aus System-Befehlen besteht, die nacheinander abgearbeitet werden. Mit dieser Datei werden nicht nur die beiden Programme gestartet, sondern davor alle verschlüsselten Dateien im aktuellen Verzeichnis gelöscht und aus dem Unterverzeichnis `backup` kopiert.

Batch-Datei mit Namen `workshop` für Linux:

```
rm -f text*
cp ./backup/text* ./
~/jcryptool/JCrypTool &
emacs &
```

Weiter auf nächster Seite

6.2 Präsenz-Workshop: Ablauf

Allgemeines: Dieser Workshop wurde im Schülerseminar in 90 Minuten durchgeführt. Die Zeit hat genau gereicht. Da nur 90 Minuten zur Verfügung standen, wurde viel auf die Arbeitsblätter geschrieben, damit die Schüler:innen wenig Zeit zum Mitschreiben brauchten.

Das Material wurde zum Teil an der Tafel, zum Teil mit Computer und Beamer und zum Teil mit einem Visualizer praesentiert, so wie im Text angegeben.

Alle für den Workshop verwendeten Dateien sind im Verzeichnis `ver` enthalten. Deshalb müssen die Schüler:innen beim Einloggen, wenn sie die konsole geöffnet haben, „`cd ver`“ eintippen.

Die Arbeitsblätter stehen im Kapitel 15 zur Verfügung. Sie unterscheiden sich leicht von den Arbeitsblättern für den online-Workshop. Insbesondere ist der Text in Aufgabe 3 ein anderer, und die Programmbeschreibungen sind verschieden.

Wenn man weiß, welche Bücher bei Schüler:innen entsprechenden Alters gerade angesagt sind, kann man Textabschnitte daraus verschlüsseln und an Stelle der vorgegebenen Texte verwenden. Mit `CrypTool` bzw. `emacs` kann man auch sehr gut verschlüsseln.

Beginn der Stunde: Zu Beginn wurde an Hand einer an der Tafel vorbereiteten Tabelle (wie auf Arbeitsblatt 1 im Abschnitt Caesar-Chiffre) das Verfahren der Caesar-Verschlüsselung erklärt. Dazu wurden die letzten vier Zuordnungen zunächst weggelassen. Dann kann man fragen, wie die Zuordnungen nach dem z weitergehen müssen, und was das mit unserem Thema zu tun hat (wir „rechnen“ modulo 26). Dann wurden die vier Zuordnungen ergänzt.

Arbeitsblatt 1: Nach Austeilen des Arbeitsblattes loggt sich L. wie angegeben ein und zeigt mit dem Beamer, wie der Bildschirm dabei aussieht. Parallel dazu loggen sich die Schüler:innen ein. Danach erklärt L. an der Tafel, wie die ersten zwei Buchstaben der Geheimbotschaft auf Seite 2 entschlüsselt werden. Den Rest entschlüsseln die Schüler:innen selber auf dem Arbeitsblatt. L. notiert anschließend die Lösung an der Tafel.
(Lösung: GUMMIBAERCHEN SCHMECKEN GUT)

Vielleicht kommt von den Schüler:innen die Frage, warum nur 25 Möglichkeiten durchprobiert werden müssen, obwohl das Alphabet 26 Buchstaben hat.

Nun Hinweis, dass man lieber ein Programm probieren lässt als dies von Hand zu tun. Auch die Entschlüsselung geht dann schneller.

L. führt vor, wie man in `CrypTool` und im `emacs` Dateien öffnet und den Entschlüsselungmodus einstellt (Beamer). Bei `text1-Caesar.txt` findet `CrypTool` problemlos die Lösung. Aber bei `text2-Caesar.txt` kommt nichts gescheites heraus. Er ist zu kurz und hat nicht die richtigen Buchstabenhäufigkeiten. Hier muss man wirklich im `emacs` herumprobieren.

Arbeitsblatt 2: L. wischt die Caesar-Verschlüsselungszeile unter dem Alphabet weg, schreibt eine beliebige Permutation drunter und erklärt, wie man verschlüsselt. Dann noch ein paar Worte zu den Häufigleitstabellen auf der Rückseite des Arbeitsblattes, und schon können die Schüler:innen mit dem Probieren loslegen. Bei Fragen bietet es sich an, die Antworten am Computer mit dem Beamer zu erklären, damit auch anderem Schüler:innen von der Antwort profitieren können. Die Texte sind verschieden schwierig zu entschlüsseln. Bei `text3` sind Abstände zwischen den Worten, das vereinfacht die Sache wesentlich. Bei `text4` sind die Wortabstände weggelassen. Dadurch ist die Entschlüsselung viel schwieriger. Um Zeit zu sparen, kann L. (nach etwas Zeit) die ersten zwei Worte des entschlüsselten Textes angeben. Diejenigen, die mit der Entschlüsselung schnell fertig sind, kann man fragen, aus welchen Büchern die Texte entnommen wurden.

Arbeitsblatt 3: L. zeigt die erste Seite mit dem Visualizer und erklärt, wie man den angegebenen Satz *Heute ist es sehr heiss* verschlüsselt: Man schreibt das Passwort unter den Klartext. Dann sucht man in der Spalte, in der oben der Klartextbuchstabe steht, die Zeile, in deren Anfang der enstprechende Buchstabe des Passwortes steht und liest den Eintrag ab. Dies ist der verschlüsselte Buchstabe. Am Beispiel:

Unter „H“ steht „p“, dann wird „H“ mit der „p“-Zeile verschlüsselt: H→w.
Unter „E“ steht „r“, dann wird dieses „E„ mit der „r“-Zeile verschlüsselt: E→v.

L. trägt die beiden fehlenden Buchstaben im Chiffretext auf dem Visualizer ein, die Schüler:innen tragen sie auf ihrem Arbeitsblatt ein.

L. weist darauf hin, dass bei diese Verschlüsselung z.B. der Buchstabe „E“ verschieden verschlüsselt wird. Das bedeutet, dass die Buchstabenhäufigkeit versteckt wird.

L. erklärt nun zunächst noch am Chiffretext, wie man entschlüsselt, wenn man das Passwort kennt. Dann wird die Entschlüsselung fragend-entwickelnd für die ersten zwei oder drei Buchstaben aus Aufgabe 3 entschlüsselt. Den Rest entschlüsseln die Schüler:innen alleine.

Nun sollte man ein Säckchen Gummibären zur Hand haben, denn der entschlüsselte Text lautet: KANN ICH BITTE EIN GUMMIBAERCHEN BEKOMMEN.

Hier kann man darauf hinweisen, dass die Verschlüsselungsmaschine Enigma etwas ähnliches gemacht hat.

Der verschlüsselte Text `text5` wurde mit dem Passwort *mathematik* verschlüsselt. Dies bekommt `CrypTool` problemlos heraus.

6.3 Hilfsmittel

`https://www.cryptool.org/de/cto/caesar/`
`https://legacy.cryptool.org/de/cto/frequency-analysis`
`https://legacy.cryptool.org/de/cto/vigenerebreak`
`https://www.cryptool.org/de/cto/vigenere/`
`https://www.gnu.org/software/emacs/download.html`
`obs` zur Erstellung der Videos am Computer
`less` Dateiname | `tr ABCDEFGHIJKLMNOPQRSTUVWXYZ abcdefghijklmnopqrstuvwxyz` zur Umwandlung von Groß- in Kleinbuchstaben

Weiter auf nächster Seite

6.4 Online-Workshop: Ablauf

a) Einführung: Heute kannst Du verschiedene Verfahren kennenlernen, wie man früher Texte verschlüsselt hat, um sie für nicht eingeweihte Personen unlesbar zu machen. Eine gängige Methode besteht darin, die Buchstaben des Alphabets durch andere zu ersetzen. Und am allereinfachsten ist es, dabei das Alphabet nur zu verschieben. Dann reicht es, dass der Empfänger weiß, um wie viele Positionen das Alphabet verschoben wurde. Dieses Verfahren heißt Caesar-Verschlüsselung, weil es wohl schon von G. J. Caesar benützt wurde.

b) Blatt 1 Erklärung an Tafel, letzte Buchstaben in der Zeile Chiffretext ergänzen, Hinweis auf Modulo-Rechnung. Die ersten zwei Buchstaben der Geheimbotschaft entschlüsseln. Den Rest entschlüsseln die Schüler:innen alleine.

---

c) Lösung an Tafel angeben (GUMMIBAERCHEN SCHMECKEN GUT).

d) Aufgabe 1 vorführen mit zugeschnittenen Alphabeten, danach mit dem Programm (ICH MAG BROT MIT HONIG UND WURST DRAUF UND DAZU MILCH MIT KAKAO).

e) Zweiter Text (`text2-Caesar.txt`) als schriftliche Aufgabe.
Hinweis: Du kannst den entschlüsselten Text einfach in die Email kopieren oder in ein Textprogramm. Falls Du ein Textprogramm benützt, bitte unbedingt als pdf exportieren.

---

f) Nachteil der Caesar-Verschlüsselung: Man muss nur 25 Möglichkeiten durchprobieren. Ist bekannt, welcher Buchstabe an Stelle von E genommen wurde, dann ist die Entschlüsselung klar. Außerdem muss man dem Empfänger mitteilen, um wie viel das Alphabet verschoben wurde. Wie kann man die Verschlüsselung verbessern, so dass die Entschlüsselung für eine nicht eingeweihte Person nicht so leicht gelingt? Man verändert die Reihenfolge der Buchstaben bei der Verschlüsselung.

g) Tafel: Erklärung der Permutationsverschlüsselung, mit Hinweis, dass die Abbildung injektiv sein muss. Hinweis: Ist bekannt, welcher Buchstabe an Stelle von E genommen wurde, dann muss man die restlichen Buchstaben immer noch entschlüsseln.

h) Hinweis auf Häufigkeitstabellen

i) Dritten Text (`text3-Permutation.txt`) mit `CrypTool` und `emacs` entschlüsseln (DUNKEL WARS DER MOND SCHIEN HELLE ...).

j) Vierter Text (`text4-Permutation.txt`) als schriftliche Aufgabe.

---

k) Nachteil der Permutationsverschlüsselung: Jeder verschlüsselte Buchstabe ist genauso häufig wie der zugehörige unverschlüsselte. Und man muss die Verschlüsselungstabelle irgendwie zum Empfänger bringen.

l) Vigenère-Verschlüsselung auf dem Arbeitsblatt erklären, erste zwei Buchstaben von Hand verschlüsseln. Hinweis: Z.B. der Buchstabe E wird verschieden verschlüsselt.

m) Vorteil der Vigenère-Verschlüsselung: Gleiche Buchstaben werden je nach Position im Text verschieden verschlüsselt. Die Verschlüsselungstabelle ist öffentlich! Aber man muss immer noch dem Empfänger das Passwort schicken.

n) Aufgabe 5 Text entschluesseln mit Passwort handy: Erste drei Buchstaben vorführen (TEX), Rest selber als schriftliche Aufgabe.

o) Aufgabe 6 (`text5-Vigenere.txt`): Entschlüsselung mit `CrypTool` vorführen (Schlüsselwort: mathematik).

p) Sechster Text (`text6-Vigenere.txt`) als schriftliche Aufgabe.

---

q) Hinweis auf nächste Einheit und Abschied

6.5 Schriftliche Aufgaben (ohne Lösungen)

Anmerkung
Beispiele für verschlüsselte Texte stehen in der Ausarbeitung dieser Einheit in Kapitel 15

Aufgabe 5.2 (*Arbeitsblatt 5.4 (Schriftliche Aufgaben), Aufgabe 1*)

Entschlüssle den Text aus der Datei `text2-Caesar.txt`.

Datei: `Kryptographie590-Caesar-Verschluesselung`

Aufgabe 5.4 (*Arbeitsblatt 5.4 (Schriftliche Aufgaben), Aufgabe 2*)

Entschlüssle den Text aus der Datei `text4-Permutation.txt`.

Datei: `Kryptographie591-Permutationsverschluesselung`

Aufgabe 5.5 (*Arbeitsblatt 5.4 (Schriftliche Aufgaben), Aufgabe 3*)

Entschlüssle mit dem Schlüsselwort „handy“ den mit Vigenère verschlüsselten Text

a e k w c l n g v a o l h h q z e y q k h c u w q w a f v

Datei: `Kryptographie592-Vigenere`

Aufgabe 5.7 (*Arbeitsblatt 5.4 (Schriftliche Aufgaben), Aufgabe 4*)

Entschlüssle den Text aus der Datei `text6-Vigenere.txt` mit Hilfe des Vigenere-Breakers.
Hinweis: Die Schlüssellänge ist 10.

Datei: `Kryptographie593-VigenereMitCrypTool`

7 Unterrichtseinheit 6: Kleiner Satz von Fermat

7.1 Vorbemerkungen

Die drei Verschlüsselungsverfahren, die wir in dieser und der nächsten Einheit kennenlernen, basieren alle darauf, dass der diskrete Logarithmus schwierig zu berechnen ist. Also darauf, dass man in großen endlichen Körpern aus der Kenntnis von a und a^e den Exponenten e nur durch Ausprobieren berechnen kann.

In dieser Einheit geht es zunächst ums Potenzieren, bevor wir den Schlüsseltausch behandeln. Die Inhalte sind: Kleiner Satz von Fermat, Primitivwurzel, Diffie-Hellman-Merkle Schlüsselaustausch.

Brüche berechnen mit Hilfe des Satzes von Fermat macht Spaß, unsere Schüler:innen haben eifrig gerechnet.

Vor dieser Doppelstunde sollte die Verschlüsselung nach Vigenère behandelt werden. Sie wird in Aufgaben zum Schlüsseltausch benützt.

7.2 Wiederholung

Vorgehen: Schüler:innen schreiben die Wiederholung nicht mit. Schüler:innen fragen, was die Aussage $a \equiv b \mod m$ bedeutet.

Tafelanschrieb

Kongruenz

$a \equiv b \mod m$ bedeutet:	z.B. modulo 12:
$b - a$ ist durch m teilbar	$13 \equiv 1 \mod 12$
	$25 \equiv 1 \mod 12$
Restklassen: $[a] = \{b \in \mathbb{Z} : b \equiv a \mod m\}$	$[1] = \{\ldots, -11, 1, 13, 25, \ldots\}$
Restklassenring $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$	$\mathbb{Z}_{12} = \big\{[0], [1], [2], \ldots, [11]\big\}$

Mündlich: Und was ist mit der Restklasse $[12]$? Die Zahl 12 ist nur ein anderer Repräsentant der Restklasse $[0]$. Es gibt in $\mathbb{Z}_{12}$ genau die 12 angeschriebenen Restklassen $[0], \ldots, [11]$.

Tafelanschrieb

Rechenoperationen:
$$\begin{aligned} [a] + [b] &= [a+b] \\ [a] \cdot [b] &= [a \cdot b] \end{aligned}$$

Ist $m = p$ Primzahl, dann ist Division möglich:

$$[x] = \frac{[a]}{[b]} \Leftrightarrow [b] \cdot [x] = [a] \text{ in } \mathbb{Z}_p$$

Anmerkung

Zur Existenz von Brüchen: Falls m keine Primzahl ist, dann gilt für die Gleichung $[b] \cdot [x] = [a]$:

- Im Fall $\mathrm{ggT}(b, m) = 1$ existiert eine eindeutige Lösung $[x] \in \mathbb{Z}_m$.
- Im Fall $\mathrm{ggT}(b, m) \geq 2$ existiert keine Lösung oder es gibt mindestens zwei verschiedene Lösungen, vgl. nicht-Existenz von Brüchen auf Seite 50.

Aufgabe 6.1 (*Arbeitsblatt 6.1 (Potenzen in $\mathbb{Z}_7$), Aufgabe 1*)

In dieser Aufgabe soll in $\mathbb{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$ gerechnet werden. Das bedeutet, dass als Ergebnisse nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ eingetragen werden sollen.

Bestimme die Potenzen $[a]^k$ in $\mathbb{Z}_7$ und trage Deine Ergebnisse in die Tabelle ein.
Hinweise: Du kannst die unten stehende Verknüpfungstabelle benützen. Wenn Du die Beziehung $[a]^{k+1} = [a] \cdot [a]^k$ verwendest, geht es leichter.

Datei: `Kryptographie60-Potenzen-in-Z7`

Lösung:

$k =$	1	2	3	4	5	6
$[2]^k =$	[2]	[4]	[1]	[2]	[4]	[1]
$[3]^k =$	[3]	[2]	[6]	[4]	[5]	[1]
$[4]^k =$	[4]	[2]	[1]	[4]	[2]	[1]
$[5]^k =$	[5]	[4]	[6]	[2]	[3]	[1]
$[6]^k =$	[6]	[1]	[6]	[1]	[6]	[1]
$[0]^k =$	[0]	[0]	[0]	[0]	[0]	[0]

> **Anmerkung**
> Eine andere Version dieser Aufgabe steht im Abschnit *Weitere Aufgaben*.

> **Anmerkung**
> Vorschlag zur Benennung der Tabellen, in denen die Potenzen stehen: Potenztabellen.

Mündlich: Fällt Euch etwas auf? Kann man hier Muster erkennen? Ein Muster ist, dass in der letzten Spalte in fast jeder Zeile die Restklasse $[1]$ steht. Würde man die Tabelle nach rechts fortsetzen, dann wiederholen sich die Einträge.

Vorgehen: Die roten Kreise werden erst später ergänzt.

> **Anmerkung**
> Die Potenztabelle wird für den kleinen Satz von Fermat und später zur Verdeutlichung der Definition von Primitivwurzeln verwendet.

7.3 Der kleine Satz von Fermat

Mündlich: Wir sehen an den Potenztabellen, dass für jede von der Restklasse $[0]$ verschiedene Restklasse $[x]$ die Beziehung $[x]^6 = [1]$ gilt. Dass dies kein Zufall ist, zeigt der nächste Satz.

Tafelanschrieb

7. Potenzen im Restklassenring

Kleiner Satz von Fermat: Sei p Primzahl, $a \in \mathbb{Z}$ kein Vielfaches von p. Dann gilt

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}_p \qquad \text{bzw.} \qquad a^{p-1} \equiv 1 \mod p.$$

Mündlich: Die beiden Gleichungen sind nur verschiedene Schreibweisen für denselben Sachverhalt.

Vorgehen: Nun werden die Restklassen $[1]$ in der letzten Spalte der Potenztabelle von $\mathbb{Z}_7$ rot umkringelt.

Mündlich: Falls a Vielfaches von p ist, gilt $[a] = [0]$. Dies entspricht der letzten Zeile der Potenztabelle in Aufgabe 6.1.

Anmerkung
Man sollte auf die Schülerfrage gefasst sein: Gibt es auch einen großen Satz von Fermat? Dies ist die fermatsche Vermutung, die inzwischen von A. Wiles bewiesen wurde: Die Gleichung $x^n + y^n = z^n$ besitzt im Fall $n \in \mathbb{N}$, $n \geq 3$ keine Lösungstripel $(x, y, z) \in \mathbb{N}_+^3$, also keine Lösungen, die nur aus positiven natürlichen Zahlen bestehen.

Mündlich: Wie kann man mit dem kleinen Satz von Fermat 2^{40} modulo 19 geschickt berechnen?

Tafelanschrieb
Beispiel: $2^{40} \equiv ? \mod 19$:
Kleiner Fermat: $2^{19-1} \equiv 1 \mod 19$
$\Rightarrow \; 2^{40} = 2^{18} \cdot 2^{18} \cdot 2^4 \equiv 1 \cdot 1 \cdot 16 = 16 \mod 19$

Mündlich: Nun beweisen wir, dass die Aussage des Satzes richtig ist.

Tafelanschrieb
Beweis: Wir untersuchen die Teilmenge
$A = \{[0a], [1a], [2a], \ldots, [(p-1)a]\}$
von $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$.

Mündlich: Teilmenge bedeutet, dass alle Elemente der Menge A auch Elemente der Menge $\mathbb{Z}_p$ sind. In der Aufzählung der Restklassen, die in der Menge A liegen, stehen eventuell andere Repräsentanten als bei den Elementen von $\mathbb{Z}_p$.

Erstaunlicherweise ist diese Menge A ganz $\mathbb{Z}_p$. Dies beweisen wir und multiplizieren dann alle ihre Elemente, die von $[0]$ verschieden sind.

Tafelanschrieb
Schritt 1: Wir beweisen, dass alle p Restklassen $[0a]$, $[1a]$, $[2a]$, $\ldots$, $[(p-1)a]$ verschieden sind.

Annahme: $[ja] = [ka]$ für zwei dieser Restklassen mit $j < k$. Dann folgt

$[0] = [ka] - [ja] = [ka - ja] = \big[(k-j)a\big] = [k-j] \cdot [a]$ mit $[k-j] \neq [0]$
$\overset{\text{Satz vom Dividieren}}{\Rightarrow} [a] = [0]$, d.h. a ist Vielfaches von $p \;\Rightarrow$ Widerspruch
Also muss $[ja] \neq [ka]$ für $j \neq k$ gelten.

Schritt 2: Die Menge A hat p verschiedene Elemente und ist Teilmenge der p-elementigen Menge $\mathbb{Z}_p$. Also sind die Mengen gleich.

Schritt 3: Es ist klar, das $[0a] = [0]$ gilt. Wir entfernen nun dieses Element aus beiden Mengen. Das Produkt der restlichen Elemente muss gleich sein:

$$\begin{array}{rrcl} & [a] \cdot [2a] \cdot [3a] \cdots [(p-1)a] & = & [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \Leftrightarrow & [1] \cdot [2] \cdot [3] \cdots [p-1] \cdot [a]^{p-1} & = & [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \overset{\text{Satz vom Dividieren}}{\Rightarrow} & [a]^{p-1} = [1] \text{ in } \mathbb{Z}_p. & & \square \end{array}$$

Tafelanschrieb
Satz (Brüche berechnen): Sei p eine Primzahl und $[a] \in \mathbb{Z}_p$, $[a] \neq [0]$. Dann gelten:

1) $\dfrac{[1]}{[a]} \overset{\text{Kleiner Fermat}}{=} \dfrac{[a]^{p-1}}{[a]} = [a]^{p-2}$,

2) $\dfrac{[1]}{[a]^k} = \dfrac{[a]^{p-1}}{[a]^k} = [a]^{p-1-k}$ für $k = 1, 2, \ldots, p-2$.

Brüche können also durch Potenzen berechnet werden.

Mündlich: Zur Berechnung von Brüchen in $\mathbb{Z}_p$ kann diese Methode nicht hoch genug geschätzt werden. Bisher konnten wir Brüche nur durch Ablesen in der Multiplikationstabelle bestimmen oder durch Lösen diophantischer Gleichungen.

> **Anmerkung**
> Es gilt $[a]^{p-1} = [1]$ und $[a+p] = [a]$. Es kann leicht verwechselt werden, wann p bzw. $p-1$ verwendet werden muss. Ein häufiger Fehler ist, dass Schüler:innen den Exponenten p an Stelle von $p-1$ verwenden.

Aufgabe 6.2 (*Arbeitsblatt 6.2 (Brüche berechnen), Aufgabe 2*)

Berechne die folgenden Brüche jeweils im angegebenen Restklassenring.

a) $\frac{[1]}{[5]^{20}}$ in $\mathbb{Z}_{23}$: $\quad \frac{[1]}{[5]^{20}} = [5]^{23-1-20} = [5]^2 = [25] = [2]$

b) $\frac{[13]}{[5]^{20}}$ in $\mathbb{Z}_{23}$: $\quad \frac{[13]}{[5]^{20}} = [13] \cdot \frac{[1]}{[5]^{20}} = [13] \cdot [2] = [26] = [3]$

c) $\frac{[1]}{[4]^6}$ in $\mathbb{Z}_{13}$: $\quad \frac{[1]}{[4]^6} = \frac{[4]^{12}}{[4]^6} = [4]^6 = \left([4]^2\right)^3 = [16]^3 = [3]^3 = [27] = [1]$

oder $\quad \frac{[1]}{[4]^6} = \frac{[1]}{[2]^{12}} = \frac{[1]}{[1]} = [1]$

d) $\frac{[10]}{[4]^5}$ in $\mathbb{Z}_{13}$: $\quad \frac{[10]}{[4]^5} = \frac{[10]\cdot[4]}{[4]^6} \overset{\text{Teil c)}}{=} [10]\cdot[4]\cdot[1] = [40] = [1]$

Datei: `Kryptographie61-Brueche`

Lösung: Ist bereits im Text enthalten.

Aufgabe 6.3 (*Arbeitsblatt 6.2 (Brüche berechnen), Zusatzaufgabe 1*)

Bestimme jeweils alle Lösungen der angegebenen Gleichung.

a) $[2] \cdot [x] = [5]$ in $\mathbb{Z}_7$,

b) $2 \cdot x \equiv 5 \mod 7$,

c) $4 \cdot x \equiv 3 \mod 11$.

Datei: `Kryptographie62-Kongruenzgleichungen`

Lösung: **a)** $[x] = \frac{[5]}{[2]} = [5] \cdot \frac{[1]}{[2]} = [5] \cdot [2]^{7-2} = [5] \cdot [32] = [5 \cdot 4] = [20] = [6]$,

b) Aus a): $x \equiv 6 \mod 7$, d.h. $x \in \{\ldots, -8, -1, 6, 13, \ldots\}$,

c) $4 \cdot x \equiv 3 \equiv 3 \cdot 4^{10} \mod 11$
$\Rightarrow \; x \equiv 3 \cdot 4^9 = 3 \cdot 64^3 \equiv 3 \cdot 9^3 = 27 \cdot 81 \equiv 5 \cdot 4 = 20 \equiv 9 \mod 11$,
d.h. $x \in \{\ldots, -13, -2, 9, 20, \ldots\}$.

7.4 Primitivwurzeln

Tafelanschrieb

Definition: Ein Element $[g] \in \mathbb{Z}_m$ heißt Primitivwurzel, falls durch $[g]^k$ alle Elemente von $\mathbb{Z}_m$ außer $[0]$ dargestellt werden können.

Vorgehen: Wichtig ist, dass eine Beispiel-Potenztabelle im Aufschrieb steht. Deshalb wird die Potenztabelle in $\mathbb{Z}_5$ gemeinsam an der Tafel zum Mitschreiben erarbeitet.

Tafelanschrieb

Beispiel: In $\mathbb{Z}_5$:

$k =$	1	2	3	4
$[2]^k =$	$[2]$	$[4]$	$[3]$	$[1]$
$[4]^k =$	$[4]$	$[1]$		

$\Rightarrow$ $[2]$ ist eine Primitivwurzel, aber $[4]$ nicht.

Mündlich: Wie kann man an der Potenztabelle sehen, ob eine Restklasse Primitivwurzel ist?

Man berechnet die Elemente $[g]^1, \ldots, [g]^{m-1}$ der Reihe nach und hört auf, sobald sich $[1]$ ergibt. $[g]$ ist genau dann Primitivwurzel, wenn die Restklasse $[1]$ erst für $k = m-1$ auftritt. Ergibt sich $[1]$ für ein kleineres k, so wiederholen sich die Einträge und $[g]^k$ kann nicht alle $m-1$ Elemente von $\mathbb{Z}_m$ außer der $[0]$ darstellen.

Aufgabe 6.4 (*Arbeitsblatt 6.3 (Primitivwurzeln), Aufgabe 3*)

a) Bestimme mit Hilfe der Potenztabellen aus Aufgabe 1, welche Elemente von $\mathbb{Z}_7$ Primitivwurzeln sind.

Primitivwurzeln in $\mathbb{Z}_7$ sind: $[3], [5]$

Keine Primitivwurzeln in $\mathbb{Z}_7$ sind: $[2], [4], [6]$

b) Fülle für $\mathbb{Z}_{11}$ in der folgenden Potenztabelle jede Zeile so weit aus, bis Du das Element $[1]$ erhältst.

$k =$	1	2	3	4	5	6	7	8	9	10
$[10]^k =$	$[10]$	$[1]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$
$[6]^k =$	$[6]$	$[3]$	$[7]$	$[9]$	$[10]$	$[5]$	$[8]$	$[4]$	$[2]$	$[1]$
$[3]^k =$	$[3]$	$[9]$	$[5]$	$[4]$	$[1]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$	$[\ ]$
$[2]^k =$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$

c) Welche der Elemente $[10], [6], [3], [2]$ sind Primitivwurzeln?

In $\mathbb{Z}_{11}$ sind Primitivwurzeln: $[6], [2]$

Datei: `Kryptographie63-Primitivwurzeln`

Lösung: Ist bereits im Aufgabentext enthalten.

Anmerkung
Die Tabelle der Potenzen $[2]^k$ wird in Aufgabe 6.6 verwendet. Die Potenzen $[6]^k$ werden im schriftlichen Aufgabenblatt benötigt (Aufgabe 6.10).

Falls die Zeit knapp ist, kann man die letzte Aufgabe weglassen und an die Tafel schreiben, welche Elemente von $\mathbb{Z}_7$ Primitivwurzeln sind. Dann sollte die Berechnung der Potenzen von $[2]$ in $\mathbb{Z}_{11}$ in Aufgabe 6.6 extra verlangt werden.

Anmerkung
Schülerfrage: Können nur Restklassen von Primzahlen Primitivwurzeln sein? Man sieht an der letzten Aufgabe, dass auch $[6]$ eine Primitivwurzel sein kann.

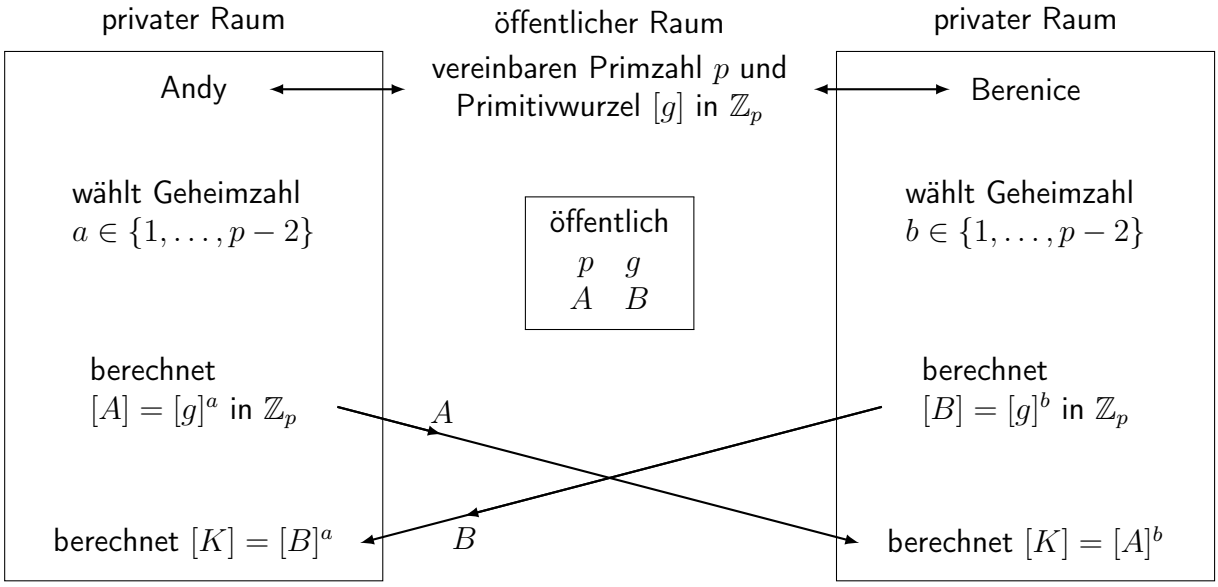
7.5 Schlüsselaustausch

Mündlich: Andy (Australien) und Berenice (Belgien) wollen sich über Whatsapp Nachrichten schicken. Da alles über einen Server läuft, haben sie Sorge, dass jemand ihre Nachrichten mitlesen könnte. Sie wollen Ihre Texte so verschlüsseln, dass niemand anderes ihre Texte verstehen kann, auch wenn alle ihre Nachrichten bekannt sind. Das bedeutet, auch die Vereinbarung ihres Schlüssels kann mitgelesen werden (sie können sich nicht treffen, um persönlich einen Schlüssel auszutauschen). Ist so eine Verschlüsselung möglich? Auch wenn ein Mathematiker oder ein Hacker versucht, Schlüssel und Nachrichten zu knacken?

Anmerkung
Der folgende Aufschrieb ist sehr breit. Tafel bzw. Heft müssen gut eingeteilt werden.

Tafelanschrieb

8. Diffie-Hellman-Merkle-Schlüsselaustausch



Andy und Berenice erhalten die selbe Schlüsselzahl K, denn es gilt

$[B]^a = \big([g]^b\big)^a = [g]^{ab} = \big([g]^a\big)^b = [A]^b$.

Mündlich: Andy und Berenice erhalten die selbe Schlüsselzahl K. Damit können sie dann Texte verschlüsseln, z.B. indem sie die Zahl K als Wort ausgeschrieben als Schlüsselwort für die Vigenère-Verschlüsselung verwenden.

Anmerkung
Die folgende Informationsbox befindet sich auf dem nächsten Arbeitsblatt.

Der Diffie-Hellman-Merkle Schlüsselaustausch:

Beide Partner vereinbaren eine Primzahl p und eine Primitivwurzel $[g]$ für $\mathbb{Z}_p$.

Andy wählt $a \in \{1, 2, \ldots, p-2\}$ und berechnet: $[A] = [g]^a$ in $\mathbb{Z}_p$
Berenice wählt $b \in \{1, 2, \ldots, p-2\}$ und berechnet: $[B] = [g]^b$ in $\mathbb{Z}_p$

Dann tauschen Sie A und B aus. Das bedeutet: (p, g, A, B) sind öffentlich bekannt,
a kennt nur Andy,
b kennt nur Berenice.

Jeder von beiden berechnet nun den gemeinsamen Schlüssel K:

Andy berechnet mit seiner Geheimzahl a: $[K] = [B]^a$ in $\mathbb{Z}_p$,
Berenice berechnet mit ihrer Geheimzahl b: $[K] = [A]^b$ in $\mathbb{Z}_p$.

Beide erhalten den selben Wert für K, denn: $[B]^a = \big([g]^b\big)^a = [g]^{ab} = \big([g]^a\big)^b = [A]^b$.

Aufgabe 6.5 (*Arbeitsblatt 6.4 (Schlüsselaustausch), Aufgabe 4*)

Andy und Berenice vereinbaren $p = 7$ und $g = 3$.

Andy wählt: $a = 3$, berechnet A: $[g]^a = [3]^3 = [27] = [6]$ in $\mathbb{Z}_7 \Rightarrow A = 6$

Berenice wählt: $b = 4$, berechnet B: $[g]^b = [3]^4 = [81] = [4]$ in $\mathbb{Z}_7 \Rightarrow B = 4$

Hinweis: A, B müssen zwischen 1 und 6 liegen.

Öffentlich bekannt sind also:

$$\boxed{p = 7,\ g = 3,\ A = 6,\ B = 4.}$$

Andy berechnet: $[B]^a = [4]^3 = [64] = [1]$ in $\mathbb{Z}_7 \Rightarrow K = 1$

Berenice berechnet: $[A]^b = [6]^4 = [36]^2 = [1]^2 = [1]$ in $\mathbb{Z}_7 \Rightarrow K = 1$

Hinweis: K muss zwischen 1 und 6 liegen.

Für Andy und Berenice kommt die selbe Zahl K als Ergebnis heraus. Schreibe diese Zahl mit Buchstaben als Wort und verwende dieses Zahlwort als Schlüsselwort für die Vigenère-Entschlüsselung, um die Nachricht `izqtimew` zu entschlüsseln.

Verschlüsselt	i	z	q	t	i	m	e	w
Schlüssel	e	i	n	s	e	i	n	s
Nachricht	E	R	D	B	E	E	R	E

Datei: `Kryptographie64-Schluesseltausch`

Lösung: Ist bereits im Aufgabentext enthalten.

Aufgabe 6.6 (*Arbeitsblatt 6.4 (Schlüsselaustausch), Zusatzaufgabe 2*)

Andy und Berenice vereinbaren $p = 11$ und $g = 2$. Andy schickt an Berenice die Zahl $A = 5$, Berenice meldet $B = 8$. Kurze Zeit später übermittelt Andy die Nachricht

h	i	x	y	z	q	w	k	n	c	t	v	m
v	i	e	r	v	i	e	r	v	i	e	r	v
M	A	T	H	E	I	S	T	S	U	P	E	R

Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[2]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).

Anmerkung: Die Verschlüsselung kann hier geknackt werden, da für p, g, a, b kleine Zahlen verwendet wurden. In der richtigen Anwendung werden sehr große Zahlen verwendet. Dann ist es schwierig, aus g und A die Zahl a zu berechnen.

Datei: `Kryptographie65-Schluesseltausch`

Lösung: Aus $A = 5$ und $[2]^a = [5]$ liest man aus der Tabelle $a = 4$ ab.

Aus $B = 8$ und $[2]^b = [8]$ liest man aus der Tabelle $b = 3$ ab.

$\Rightarrow\ A^b = 5^3 = 125 \equiv 125 - 121 = 4 \mod 11 \ \Rightarrow\ K = 4.$

Entschlüsselung siehe Aufgabentext.

> **Anmerkung**
> Das Verfahren funktioniert auch, wenn g keine Primitivwurzel ist. Man wählt g als Primitivwurzel, um möglichst viele verschiedene Schlüssel K zu erreichen. Andernfalls kann die Aufgabe, aus $A \equiv g^a \mod p$ auf a zu schließen, leichter gelöst werden.

7.6 Schriftliche Aufgaben (ohne Lösungen)

Aufgabe 6.7 (*Arbeitsblatt 6.5 (Schriftliche Aufgaben), Aufgabe 5*)

Berechne jeweils die Potenz in dem angegebenen Restklassenring $\mathbb{Z}_m$. Beachte, dass der kleine Satz von Fermat dann und nur dann angewandt werden kann, wenn m eine Primzahl ist.

a) In $\mathbb{Z}_{29}$: $[4]^{28} =$ ☐,

b) in $\mathbb{Z}_{31}$: $[17]^{94} =$ ☐,

c) in $\mathbb{Z}_{12}$: $[4]^{11} =$ ☐,

d) in $\mathbb{Z}_{12}$: $[3]^{12} =$ ☐.

Datei: `Kryptographie690-Potenzen`

Aufgabe 6.8 (*Arbeitsblatt 6.5 (Schriftliche Aufgaben), Aufgabe 6*)

a) Berechne die angegebenen Potenzen in $\mathbb{Z}_{13}$ und trage sie in die Tabelle ein.

Hinweis: Es dürfen nur Zahlen von 0 bis 12 eingetragen werden. Sobald die Restklasse $[1]$ erreicht ist, brauchst Du nichts mehr einzutragen.

$k =$	1	2	3	4	5	6
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

b) Welche der Restklassen $[2], [3], [4], [5]$ sind Primitivwurzeln?

In $\mathbb{Z}_{13}$ sind Primitivwurzeln: ☐.

Datei: `Kryptographie692-Primitivwurzeln-Z13`

Aufgabe 6.9 (*Arbeitsblatt 6.5 (Schriftliche Aufgaben), Aufgabe 7*)

a) Berechne in $\mathbb{Z}_{23}$ die angegebenen Brüche:

$\frac{[2]}{[3]^{20}} =$ ☐,

$\frac{[5]}{[9]^{11}} =$ ☐.

b) Gib jeweils 4 verschiedene Werte für k an, so dass die angegebene Gleichung in $\mathbb{Z}_{31}$ gilt. Genau einer der k-Werte soll negativ sein.

$[7]^k = [7]^3$ für $k =$ ☐,

$[16]^k = [16]^2$ für $k =$ ☐,

Datei: `Kryptographie691-Brueche-Potenzen`

Aufgabe 6.10 (*Arbeitsblatt 6.5 (Schriftliche Aufgaben), Aufgabe 8*)

Andy und Berenice vereinbaren für den Schlüsseltausch $p = 11$ und $g = 6$. Andy schickt an Berenice die Zahl $A = 8$, Berenice meldet $B = 2$. Kurze Zeit später übermittelt Andy die Nachricht

k	m	l	s	k	h	l	o	i	n	e	p	z	b

a) Bestimme a, b und den Schlüssel K.

$a =$ ☐, $b =$ ☐, $K =$ ☐.

b) Entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[6]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).

Datei: `Kryptographie693-Schluesseltausch`

7.7 Ergänzung: Negativer Primzahltest

Aufgabe 6.11 (*Arbeitsblatt 6.Arbeitsblatt, Aufgabe, Aufgabe 9*)

Für die Zahl $m \in \mathbb{N}$ soll gezeigt werden, dass sie keine Primzahl ist. Falls wir ein $a \in \mathbb{N}$ finden, so dass $a^{m-1} \not\equiv 1 \mod m$, ist m keine Primzahl. Man sagt, a ist Zeuge gegen die Primalität von m.

Beispiel: $m = 15$: $2^{14} = 16^3 \cdot 4 \equiv 1^3 \cdot 4 = 4 \mod 15$. Also ist 2 Zeuge gegen die Primalität von 15.

Aufgabe: Finde einen Zeugen gegen die Primalität von

a) $m = 21$,

b) $m = 25.$,

Datei: `Kryptographie698-NegativerPrimzahltest`

Lösung: **a)** Lösung: 2 ist Zeuge, denn
$2^{20} \overset{2^5=32}{=} 32^4 \overset{32\equiv 11}{\equiv} 11^4 = 121^2 \overset{121\equiv 16}{\equiv} 16^2 = 256 \equiv 46 \equiv 4 \mod 21$.

b) Lösung: 2 ist Zeuge, denn
$2^{24} \overset{2^5=32}{=} 32^4 \cdot 16 \overset{32\equiv 7}{\equiv} 7^4 \cdot 16 = 49^2 \cdot 16 \overset{49\equiv -1}{\equiv} (-1)^2 \cdot 16 = 16 \mod 25$.

7.8 Ergänzung: Eigenschaften von Primitivwurzeln

Satz: Sei p eine Primzahl. Dann gilt für $[a] \in \mathbb{Z}_p$ mit $[a] \neq [0]$: $[a]$ ist genau dann Primitivwurzel, wenn $[a]^k \neq [1]$ für $k = 1, 2, \ldots, p-2$.

Beweis: Nach dem kleinen Satz von Fermat gilt $[a]^{p-1} = [1]$. Betrachte die Menge $P([a]) := \{[a]^1, [a]^2, \ldots, [a]^{p-2}, [a]^{p-1} = [1]\}$. Diese Menge hat genau dann $p-1$ Elemente, wenn in der Aufzählung alle Elemente verschieden sind. Die Menge $\mathbb{Z}_p \setminus \{0\}$ hat genau $p-1$ Elemente.

a) Falls $[a]^k = [1]$ für ein $k \leq p-2$, dann hat $P([a])$ weniger Elemente als $\mathbb{Z}_p \setminus \{0\}$. Also ist $[a]$ keine Primitivwurzel.

b) Falls $[a]^k \neq [1]$ für $k \leq p-2$, dann sind alle Elemente von $P([a])$ verschieden, also ist $[a]$ Primitivwurzel.

Denn sind zwei Elemente von $P([a])$ gleich: $[a]^k = [a]^j$ mit $k > j$, so folgt mit dem Satz vom Dividieren

$$[a]^{k-j} = [a]^k \cdot \frac{1}{[a]^j} = [a]^j \cdot \frac{1}{[a]^j} = [1].$$

Nun gilt $[a]^{k-j} = [1]$ mit $k - j < k \leq p-1$, also $k - j \leq p-2$. Widerspruch! □

Anmerkung
Ist p eine Primzahl, so existiert in $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ immer mindestens eine Primitivwurzel. Aber Primitivwurzeln zu finden, ist nicht einfach. Hilfen bei der Suche:

a) $[g] \in \mathbb{Z}_p$ ist genau dann eine Primitivwurzel, wenn $[g]^k \neq [1]$ für alle $k = 1, \ldots, p-2$.

b) Für jedes $[a] \in \mathbb{Z}_p$ gelten:

- $[a]^k = [1] \;\Rightarrow\; \mathrm{ggT}(k, p-1) \geq 2$,
- Ist K der kleinste Exponent, für den $[a]^K = [1]$ gilt, so ist K ein Teiler von $p-1$.

c) Ist $[g] \in \mathbb{Z}_p$ eine Primitivwurzel (bezüglich Multiplikation), dann sind genau alle $[g]^k$ ebenfalls Primitivwurzeln, für die $\mathrm{ggT}(k, p-1) = 1$ gilt. Mit dieser Methode kann man aus einer Primitivwurzel alle anderen Primitivwurzeln in $(\mathbb{Z}_p, \cdot)$ konstruieren.

d) Ist $\frac{p-1}{2} = q$ ebenfalls eine Primzahl (p heißt dann sichere Primzahl), dann gilt:
$[a]^2 \neq [1] \;\wedge\; [a]^q \neq [1] \;\Rightarrow\; [a]$ ist Primitivwurzel in $(\mathbb{Z}_p, \cdot)$.

e) Zum Test, ob $[g] \in \mathbb{Z}_p$ eine Primitivwurzel ist, reicht es, die Bedingung $[g]^k \neq [1]$ für alle Teiler k von $p-1$ zu überprüfen (siehe 2)). Das bedeutet, man muss nur $[g]^k \neq [1]$ für $k = 1, 2, \ldots, T$ überprüfen, wobei T den größten Teiler von $p-1$ bezeichnet.

f) Quadratzahlen können keine Primitivwurzeln sein: Wegen $[n]^{p-1} = [1]$ nach dem kleinen Fermat gilt $[n^2]^{(p-1)/2} = [1]$ mit $\frac{p-1}{2} \in \mathbb{N}$ und $\frac{p-1}{2} < p-1$, und nach dem letzten Satz kann $[n^2]$ keine Primitivwurzel sein.

7.9 Weitere Aufgaben

Aufgabe 6.12 (*Arbeitsblatt 6.6 (Zusatzaufgaben), Aufgabe 10*)

In dieser Aufgabe soll in $\mathbb{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$ gerechnet werden. Das bedeutet, dass als Ergebnisse nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ eingetragen werden sollen.

a) Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_7$ aus (z.B. $[3] \cdot [4] = [12] = [12 - 7] = [5]$):

b) Lies aus der Tabelle aus a) die Potenzen von $[2]$ und $[3]$ ab und trage sie in die Tabelle ein.
Hinweis: Wenn Du die Beziehung $[a]^{k+1} = [a] \cdot [a]^k$ verwendest, geht es leichter.

c) **Zusatzaufgabe:** Trage in die Tabelle die Potenzen $[4]^k, [5]^k, [6]^k, [0]^k$ ein.

Datei: `Kryptographie695-Multiplizieren-in-Z7`

Lösung: **a)**

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$
$[3]$	$[0]$	$[3]$	$[6]$	$[2]$	$[5]$	$[1]$	$[4]$
$[4]$	$[0]$	$[4]$	$[1]$	$[5]$	$[2]$	$[6]$	$[3]$
$[5]$	$[0]$	$[5]$	$[3]$	$[1]$	$[6]$	$[4]$	$[2]$
$[6]$	$[0]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

b)

$k =$	1	2	3	4	5	6
$[2]^k =$	$[2]$	$[4]$	$[1]$	$[2]$	$[4]$	$[1]$
$[3]^k =$	$[3]$	$[2]$	$[6]$	$[4]$	$[5]$	$[1]$

c)

$k =$	1	2	3	4	5	6
$[4]^k =$	$[4]$	$[2]$	$[1]$	$[4]$	$[2]$	$[1]$
$[5]^k =$	$[5]$	$[4]$	$[6]$	$[2]$	$[3]$	$[1]$
$[6]^k =$	$[6]$	$[1]$	$[6]$	$[1]$	$[6]$	$[1]$
$[0]^k =$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$

Aufgabe 6.13 (*Arbeitsblatt 6.6 (Zusatzaufgaben), Aufgabe 11*)

Berechne in $\mathbb{Z}_{23}$ die folgenden Brüche:

a) $\dfrac{[1]}{[5]^{21}}$, **b)** $\dfrac{[1]}{[10]^{13}}$, **c)** $\dfrac{[7]}{[10]^{12}}$, **d)** $\dfrac{[7]}{[21]}$.

Hinweis: Benutze in der letzten Teilaufgabe, dass $[21] = [-2]$ gilt.

Datei: `Kryptographie66-Brueche-Z23`

Lösung: **a)** $\dfrac{[1]}{[5]^{21}} = [5]^{23-1-22} = [5]$,

b) $\dfrac{[1]}{[10]^{13}} = [10]^9 \overset{\text{Taschenrechner}}{=} [20]$,

Alternative Lösung von Hand: $[10]^2 = [100] = [100 - 4 \cdot 23] = [8]$
$\Rightarrow\ [10^4] = [64] = [64 - 3 \cdot 23] = [-5]\ \Rightarrow\ [10^8] = [25] = [2]\ \Rightarrow\ [10^9] = [20]$

c) $\dfrac{[7]}{[10]^{12}} = [7] \cdot [10] \cdot \dfrac{[1]}{[10]^{13}} \overset{\text{Teil b)}}{=} [70] \cdot [20] = [70 - 3 \cdot 23] \cdot [20] = [1] \cdot [20] = [20],$

d) $\dfrac{[7]}{[21]} = \dfrac{[7]}{[-2]} = [7] \cdot [-2]^{21} = [7] \cdot [-1] \cdot [2] \cdot [32]^4 = [-14] \cdot [9]^4$
$= [9] \cdot [81]^2 = [9] \cdot [12]^2 = [9] \cdot [144] = [9] \cdot [6] = [54] = [8].$

Aufgabe 6.14 (*Arbeitsblatt 6.6 (Zusatzaufgaben), Aufgabe 12*)

Gegeben ist die diophantische Gleichung

$$25x + 17y = 5.$$

a) Eliminiere die Variable y, indem Du die Gleichung als Kongruenz-Gleichung (modulo 17) schreibst.

b) Berechne alle Werte für x durch Lösung der Kongruenz-Gleichung.

c) Berechne alle Lösungen $(x \mid y)$.

Datei: `Kryptographie67-Diophantisch-Kongruenz`

Lösung: **a)** $25 \cdot x \equiv 5 \mod \mod 17.$

b) in $\mathbb{Z}_{17}$: $[25] \cdot [x] = [5]$
$\Rightarrow\ [x] = \dfrac{[5]}{[25]} = \dfrac{[5]}{[8]} = [5] \cdot [8]^{15} = [5] \cdot \left([8]^5\right)^3 \overset{\text{Taschenrechner}}{=} [5] \cdot [9]^3 \overset{\text{Taschenrechner}}{=} [7].$
$[x] = [7]\ \Rightarrow\ x = 7 + k \cdot 17$

c) $17y = 5 - 25x = 5 - 25(7 + k \cdot 17) = -170 - k \cdot 25 \cdot 17$
$\Rightarrow\ y = -10 - k \cdot 25$
$\Rightarrow$ Alle Lösungen: $(x \mid y) = \left(7 + k \cdot 17 \mid -10 - k \cdot 25\right)$ mit $k \in \mathbb{Z}$.

Aufgabe 6.15 (*Arbeitsblatt 6.6 (Zusatzaufgaben), Aufgabe 13*)

Stelle fest, welche der Elemente von $\mathbb{Z}_p$ Primitivwurzeln sind. Trage in die Tabelle „J“ für Ja bzw. „N“ für Nein ein:

a) In $\mathbb{Z}_7$:

$[n]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[n]$ ist Primitivwurzel	N	N	J	N	J	N

b) In $\mathbb{Z}_{11}$:

$[n]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[n]$ ist Primitivwurzel	N	J	N	N	N	J	J	J	N	N

Datei: `Kryptographie68-Primitivwurzeln`

Lösung: Ist bereits im Aufgabentext enthalten.

Aufgabe 6.16 (*Arbeitsblatt 6.6 (Zusatzaufgaben), Aufgabe 14*)

In dieser Aufgabe rechnen wir in $\mathbb{Z}/11\mathbb{Z}$.

a) Stelle eine Tabelle auf, in der alle Potenzen $[2]^k$ mit $k = 1, 2, \ldots, 10$ aufgeführt sind. Ist $[2]$ eine Primitivwurzel?

b) Berechne den Bruch $\dfrac{[7]}{[8]}$, indem Du $[7]$ als Potenz $[2]^k$ (k aus der Tabelle ablesen) und entsprechend $[8]$ als Potenz von $[2]$ darstellst.

c) Bestimme für alle $[a] \in \mathbb{Z}/13\mathbb{Z}$ mit $[a] \neq 0$ das inverse Element $[a]^{-1}$.
Hinweis: Verfahre entsprechend zu Teil b) und verwende den kleinen Fermat.

Datei: `Kryptographie697-RechnenMitFermat`

Lösung: **a)**

$k =$	1	2	3	4	5	6	7	8	9	10
$[2]^k =$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$

b) $\dfrac{[7]}{[8]} \overset{\text{Tabelle}}{=} \dfrac{[2]^7}{[2]^3} = [2]^4 \overset{\text{Tabelle}}{=} [5]$

c) $[2]^{-1} = [2]^9 = [6]$, $[3]^{-1} = [2]^{-8} = [2]^2 = [4]$, $[4]^{-1} = [2]^{-2} = [2]^8 = [3]$,
$[5]^{-1} = [2]^{-4} = [2]^6 = [9]$, $[6]^{-1} = [2]^{-9} = [2]^1 = [2]$, $[7]^{-1} = [2]^{-7} = [2]^3 = [8]$,
$[8]^{-1} = [2]^{-3} = [2]^7 = [7]$, $[9]^{-1} = [2]^{-6} = [2]^4 = [5]$, $[10]^{-1} = [2]^{-5} = [2]^5 = [10]$.

8 Unterrichtseinheit 7: Asymmetrische Verschlüsselung

8.1 Vorbemerkungen

Inhalte: Elgamal-Verschlüsselung, Kongruenzgleichungen, RSA-Verfahren.

8.2 Wiederholung

Vorgehen: Schüler:innen schreiben Wiederholung nicht mit. An der Tafel steht bereits die Potenztabelle für $\mathbb{Z}_7$. Die roten Kreise werden erst nachträglich zur Erklärung des kleinen Fermats ergänzt.

Tafelanschrieb

Potenztabelle für $\mathbb{Z}_7$:

$k=$	1	2	3	4	5	6
$[0]^k=$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]^k=$	$[1]$	$[1]$	$[1]$	$[1]$	$[1]$	$[1]$
$[2]^k=$	$[2]$	$[4]$	$[1]$	$[2]$	$[4]$	$[1]$
$[3]^k=$	$[3]$	$[2]$	$[6]$	$[4]$	$[5]$	$[1]$
$[4]^k=$	$[4]$	$[2]$	$[1]$	$[4]$	$[2]$	$[1]$
$[5]^k=$	$[5]$	$[4]$	$[6]$	$[2]$	$[3]$	$[1]$
$[6]^k=$	$[6]$	$[1]$	$[6]$	$[1]$	$[6]$	$[1]$

Mündlich: Welche der Restklassen ist eine Primitivwurzel in $\mathbb{Z}_7$? Wie erkennt man das?

Tafelanschrieb

Primitivwurzel: Z.B. in $\mathbb{Z}_7$: $[3], [5]$.

Kleiner Satz von Fermat: Ist p Primzahl, $[a] \neq [0]$ in $\mathbb{Z}_p$, dann

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}_p.$$

Brüche berechnen: Sei p eine Primzahl und $[a] \neq [0]$ in $\mathbb{Z}_p$. Dann gilt

$$\frac{[1]}{[a]^k} = \frac{[a]^{p-1}}{[a]^k} = [a]^{p-1-k}.$$

> **Anmerkung**
> Die andere Formulierung des kleinen Fermat ($a^{p-1} \equiv 1 \mod p$) wurde hier weggelassen, sie wird später beim Nachweis, dass das RSA-Verfahren funktioniert, aufgeschrieben.

Aufgabe 7.1 (*Arbeitsblatt 7.1 (Potenzen und kleiner Satz von Fermat), Aufgabe 1*)

Berechne die folgenden Potenzen möglichst geschickt ohne Taschenrechner:

a) $[4]^{-11}$ in $\mathbb{Z}_{13}$: $[4]^{-11} = [4]^{12-11} = [4]$

b) $[6]^{31}$ in $\mathbb{Z}_{29}$: $[6]^{31} = [6]^{28+3} = [6]^3 = [36] \cdot [6] = [36-29] \cdot [6] = [7 \cdot 6] = [42-29] = [13]$

c) $[6]^{32}$ in $\mathbb{Z}_{29}$: $[6]^{32} = [6]^{31} \cdot [6] \overset{\text{b)}}{=} [13] \cdot [6] = [78-58] = [20]$

Datei: `Kryptographie70-Potenzen-mit-Fermat`

Lösung: Ist bereits im Aufgabentext enthalten.

Aufgabe 7.2 (*Arbeitsblatt 7.1 (Potenzen und kleiner Satz von Fermat), Zusatzaufgabe 1*)

Für diese Aufgabe benützen wir eine Potenztabelle für $\mathbb{Z}_{11}$.

$k =$	1	2	3	4	5	6	7	8	9	10
$[2]^k =$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$
$[4]^k =$	$[4]$	$[5]$	$[9]$	$[3]$	$[1]$	$[4]$	$[5]$	$[9]$	$[3]$	$[1]$

a) Trage in die Tabelle die Potenzen von $[4]$ in $\mathbb{Z}_{11}$ ein. Wie viele verschiedene Elemente von $\mathbb{Z}_{11}$ können durch $[4]^k$ dargestellt werden? Warum ist $[4]$ keine Primitivwurzel?

b) Wie hängen die Zeile für $[4]^k$ und die Zeile für $[2]^k$ zusammen?

c) Sei p eine Primzahl mit $p \geq 3$ und $[n^2]$ eine Quadratzahl in $\mathbb{Z}_p$ mit $[n] \neq 0$. Folgere aus dem kleinen Satz von Fermat dass $[n^2]^{(p-1)/2} = [1]$ gilt.

d) Sei p eine Primzahl mit $p \geq 3$. Wie viele verschiedene Elemente von $\mathbb{Z}_p$ können höchstens durch $[n^2]^k$ mit $k \in \mathbb{N}$ dargestellt werden? Warum ist $[n^2]$ keine Primitivwurzel?

Datei: `Kryptographie71-Quadratzahl-keine-Primitivwurzel`

Lösung: **a)** Für die Potenzen $[4]^k$ siehe die Tabelle im Aufgabentext. Durch $[4]^k$ können 5 verschiedene Elemente von $\mathbb{Z}_{11}$ dargestellt werden. Da $\mathbb{Z}_{11}$ ohne $[0]$ mehr Elemente besitzt (nämlich 10), ist $[4]$ keine Pimitivwurzel.

b) Wenn man aus der Zeile für $[2]^k$ alle ungeraden Potenzen streicht, erhält man die Einträge für $[4]^k$.

Oder graphisch:

$k =$	1	2	3	4	5	6	7	8	9	10
$[2]^k =$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$
$[4]^k =$	$[4]$	$[5]$	$[9]$	$[3]$	$[1]$					

c) Kleiner Satz von Fermat $\Rightarrow$ $[n]^{p-1} = [1]$

Da p ungerade ist, folgt $\frac{p-1}{2} \in \mathbb{N}$

$\Rightarrow$ $[n^2]^{(p-1)/2} = \left([n]^2\right)^{(p-1)/2} = [n]^{2(p-1)/2} = [n]^{p-1} = [1]$

d) $[n^2]^{(p-1)/2} = [1]$ $\Rightarrow$ nach der Potenz $k = \frac{p-1}{2}$ wiederholen sich die Einträge:

k	1	2	$\ldots$	$\frac{p-1}{2}$	$\frac{p-1}{2}+1$	$\frac{p-1}{2}+2$	$\ldots$	$p-1$
$[n^2]^k$	$[n^2]$	$[n^2]^2$	$\ldots$	$[1]$	$[n^2]$	$[n^2]^2$	$\ldots$	$[1]$

$\Rightarrow$ durch $[n^2]^k$ können höchstens $\frac{p-1}{2}$ verschiedene Elemente von $\mathbb{Z}_p$ dargestellt werden

$\mathbb{Z}_p$ ohne die Restklasse $[0]$ hat $p-1$ Elemente

$p - 1 > \frac{p-1}{2}$ $\Rightarrow$ durch $[n^2]^k$ können nicht alle Elemente von $\mathbb{Z}_p$ ohne die Restklasse $[0]$ dargestellt werden

$\Rightarrow$ $[n^2]$ ist keine Primitivwurzel.

8.3 Elgamal-Verschlüsselung

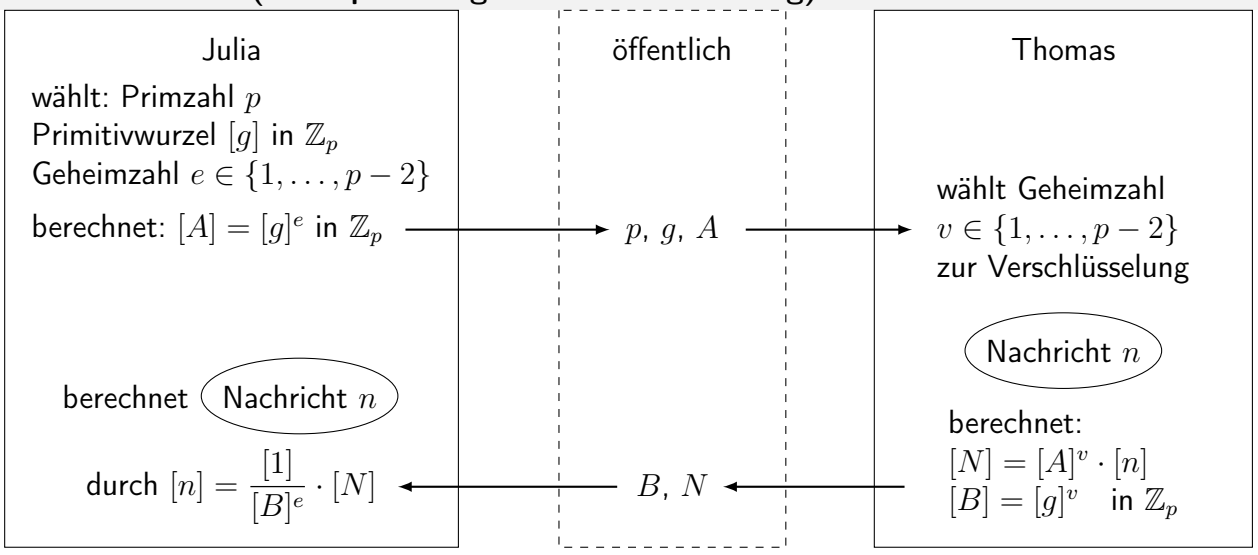
Anmerkung
Sprich: Aldschamal

Die Elgamal-Verschlüsselung ist eine Kombination von Diffie-Hellman-Merkle Schlüsseltausch und Verschlüsselung einer Nachricht durch Multiplikation in einem geeigneten Restklassenring.

Mündlich: Julia möchte Nachrichten bekommen, die von anderen Personen verschlüsselt werden, so dass nur Julia die Nachricht entschlüsseln kann. Dazu veröffentlicht sie drei Zahlen auf ihrer Homepage. Thomas kann nun eine Nachricht n verschlüsseln und an Julia schicken. Nur Julia kann die Nachricht entschlüsseln.

Vorgehen: L. teilt das Arbeitsblatt 7.2 aus und bespricht das Verfahren am Visualizer. Schüler:innen ergänzen die Begründung.

Arbeitsblatt 7.2 (Prinzip der Elgamal-Verschlüsselung)



Begründung:

$$\begin{aligned} \frac{[1]}{[B]^e} \cdot [N] &= \frac{[1]}{[B]^e} \cdot [A]^v \cdot [n] \\ &= \frac{[1]}{\left([g]^v\right)^e} \cdot \left([g]^e\right)^v \cdot [n] \\ &= \frac{[1]}{[g]^{ve}} \cdot [g]^{ev} \cdot [n] \\ &= [n] \text{ in } \mathbb{Z}_p. \end{aligned}$$

Mündlich: Julia muss die Zahl e geheim halten. Ohne Kenntnis von e kann N nicht entschlüsselt werden.

Die Entschlüsselung funktioniert, weil $\left([g]^v\right)^e = \left([g]^e\right)^v$ ist. Dies ist die selbe Begründung wie beim Schlüsseltausch von Diffie-Hellman-Merkle.

Anmerkung
Julia schickt ihren Entschlüsselungsexponenten e verschlüsselt als A, genauso schickt Thomas seinen Verschlüsselungsexponenten v verschlüsselt als B.

Da alle Rechnungen in $\mathbb{Z}_p$ geführt werden, können nur Nachrichten n zwischen 1 und p korrekt entschlüsselt werden.

Aufgabe 7.3 (*Arbeitsblatt 7.3 (Elgamal-Verschlüsselung), Aufgabe 2*)

Julia wählt $p = 23$ und die Primitivwurzel $[5]$ in $\mathbb{Z}_{23}$. Weiter wählt sie den Entschlüsselungsexponent $e = 14$ und berechnet

$$[A] = [5]^{14} = [25]^7 = [25-23]^7 = [2]^7 = [128] = [128-115] = [13] \text{ in } \mathbb{Z}_{23}.$$

Julia veröffentlicht auf ihrer Homepage $(p, g, A) = (23, 5, 13)$.

a) Thomas möchte die Nachricht $n = 11$ an Julia senden. Dazu wählt er den Verschlüsselungsexponent $v = 3$ und berechnet in $\mathbb{Z}_{23}$

$$[B] = [g]^v = [5]^3 = [125-115] = [10] \quad \text{in } \mathbb{Z}_{23},$$
$$[A]^v = [13]^3 = [169-161]\cdot[13] = [8]\cdot[13] = [104-92] = [12] \quad \text{in } \mathbb{Z}_{23},$$
$$[N] = [A]^v \cdot [n] = [12]\cdot[11] = [132-115] = [17] \quad \text{in } \mathbb{Z}_{23}.$$

Thomas schickt also $(B = 10\,, N = 17\,)$ an Julia.

Julia berechnet als erstes $[B]^{-14} = [B]^{22-14} = [B]^8 = [B^2]^4 = [B^2-92]^4 =$

$$= [100-92]^4 = [8]^4 = [64-46]^2 = [18]^2 = [-5]^2 = [25] = [2] \quad \text{in } \mathbb{Z}_{23}.$$

Hinweis: $[18] = [-5]$ kann hilfreich sein.

Dann erhält sie die Nachricht n durch Multiplikation:

$$[n] = [B]^{-14}\cdot[N] = [2]\cdot[17] = [34-23] = [11] \quad \text{in } \mathbb{Z}_{23}.$$

b) Marc schickt an Julia $(B, N) = (3, 21)$. Welche Nachricht n hat er an Julia geschickt?

$$[B]^{-14} = [B]^8 = [3]^8 = [9]^4 = [81]^2 = [81-69]^2 = [144-138] = [6] \quad \text{in } \mathbb{Z}_{23},$$
$$[n] = [6]\cdot[21] = [126] = [126-115] = [11] \quad \text{in } \mathbb{Z}_{23}.$$

c) Zusatzaufgabe: Erstelle die Potenztabelle für $[5]^k$ um herauszufinden, welchen Verschlüsselungsexponent Marc gewählt hat.

Kennzeichne Marcs Verschlüsselungsexponent durch Umkringeln.

$k =$	1	2	3	4	5	6	7	8	9	10	11
$[5]^k =$	[5]	[2]	[10]	[4]	[20]	[8]	[17]	[16]	[11]	[9]	[22]
$k =$	12	13	14	15	16	17	18	19	20	21	22
$[5]^k =$	[18]	[21]	[13]	[19]	[3]	[15]	[6]	[7]	[12]	[14]	[1]

Datei: `Kryptographie72-Elgamal`

Lösung: Ist bereits im Aufgabentext enthalten.

8.4 Lösungen von Kongruenzgleichungen

Mündlich: Für das nächste Verschlüsselungsverfahren benötigen wir Lösungen von Kongruenzgleichungen. Wir klären an einem Beispiel, wie man alle Lösungen einer Kongruenzgleichung berechnet.

Tafelanschrieb

9. Kongruenzgleichungen

Beispiel: $x \cdot 9 \equiv 1 \mod 16 \qquad (*)$

> **Anmerkung**
> Man könnte daran denken, die Gleichung als $[x] \cdot [9] = [1]$ in $\mathbb{Z}_{16}$ zu lösen. Aber der kleine Fermat ist nicht anwendbar, da $m = 16$ keine Primzahl ist. Daher müssen wir unsere Kenntnisse über diophantische Gleichungen benützen.

Mündlich: Wir verwenden eines unserer Kongruenzkriterien, um die Kongruenzgleichung zu einer Gleichung umzuformen.

Tafelanschrieb

Lösung: $(*) \Leftrightarrow 9x + 16y = 1$ für ein $y \in \mathbb{Z}$.

Mündlich: Dies ist eine diophantische Gleichung. Wir wissen, wie wir diese mit dem verallgemeinerten euklidischen Algorithmus lösen können.

Tafelanschrieb

Verallgemeinerter euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} 16 &=& 1\cdot 9 + 7 & 7 &=& 16 - 1\cdot 9 \\ 9 &=& 1\cdot 7 + 2 & 2 &=& 9 - 1\cdot 7 \\ 7 &=& 3\cdot 2 + 1 & 1 &=& 7 - 3\cdot 2 = 7 - 3(9 - 1\cdot 7) \\ & & & &=& 4\cdot 7 - 3\cdot 9 = 4(16 - 1\cdot 9) - 3\cdot 9 \\ & & & &=& 4\cdot 16 - 7\cdot 9 \end{array}$$

$\Rightarrow$ $(x, y) = (-7 \mid 4)$ ist eine Lösung.

Alle Lösungen: $(x, y) = (-7 + 16k \mid 4 - 9k)$ mit $k \in \mathbb{Z}$.

$\Rightarrow$ Alle Lösungen von $(*)$: $x = -7 + 16k$ mit $k \in \mathbb{Z}$.

Mündlich: Wir sehen: Die Kongruenzgleichung besitzt genau dann Lösungen, wenn $\mathrm{ggT}(9, 16)$ Teiler der rechten Seite der Kongruenzgleichung ist.

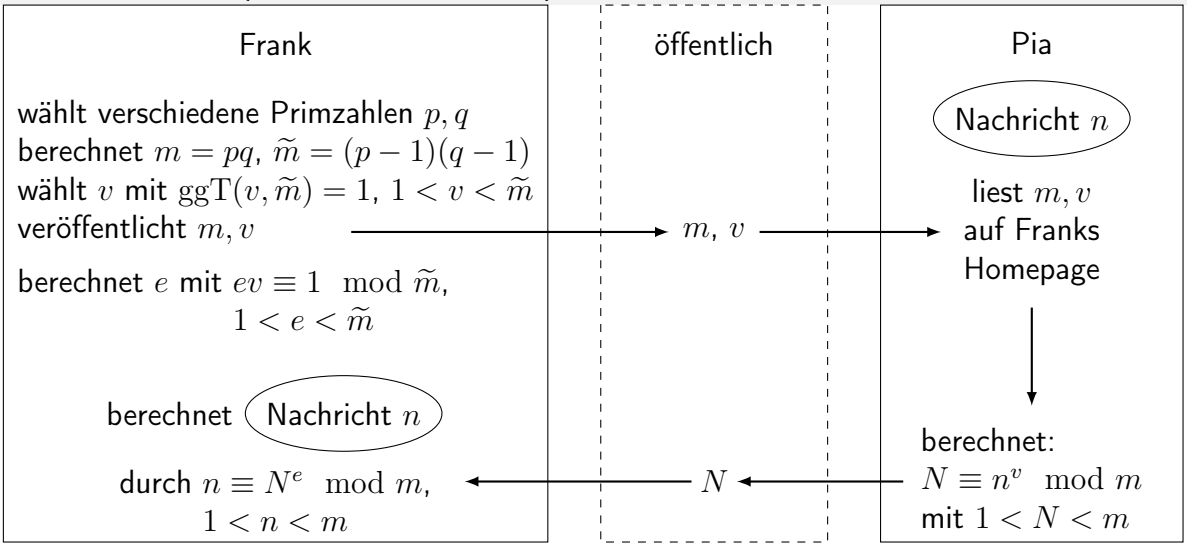
> **Anmerkung**
> Da $\mathrm{ggT}(9, 16) = 1$ gilt, sind dies alle Lösungen. Andernfalls hätte man $\frac{16}{\mathrm{ggT}(9,16)}$ anstelle von 16 und $\frac{9}{\mathrm{ggT}(9,16)}$ anstelle von 9 einsetzen müssen. Wir benötigen nur den Fall, dass der ggT der Koeffizienten 1 ist.

8.5 Das RSA-Verfahren

Mündlich: Frank schreibt auf seiner Homepage, dass er gerne Mails aus aller Welt bekommen möchte. Er hat Angst vor der CIA. Deshalb sollen die Mails gut verschlüsselt werden. Und Frank ist schlau!

Vorgehen: L. teilt das Arbeitsblatt 7.4 aus und erklärt das Verfahren am Visualizer.

Arbeitsblatt 7.4 (Das RSA-Verfahren)



Anmerkung

Ist m das Produkt zweier sehr großer Primzahlen (z.B. je 10 Stellen), dann ist es schwierig, aus m auf p, q zu schließen.

Für die Nachricht n steht im Vergleich zum Elgamal-Verfahren ein großer Zahlenraum zur Verfügung. Hier werden Nachrichten n zwischen 2 und $m = pq - 1$ ver- und entschlüsselt.

Vorgehen: Die folgende Aufgabe befindet sich auf dem selben Arbeitsblatt und wird von L. am Visualizer gelöst, Schüler:innen schreiben auf dem Arbeitsblatt mit.

Aufgabe 7.4 (*Arbeitsblatt 7.4 (Das RSA-Verfahren), Aufgabe 3*)

Frank wählt: $p = 3$, $q = 11$,

berechnet: $m = 3 \cdot 11 = 33$, $\widetilde{m} = 2 \cdot 10 = 20$,

wählt: Verschlüsselungsexponent $v = 7$ (erfüllt $1 < v < \widetilde{m}$ und $\mathrm{ggT}(v, \widetilde{m}) = 1$)

veröffentlicht: $m = 33$ und $v = 7$

berechnet: e: mit $7e \equiv 1 \mod 20$, d.h. $\mathbf{7}e + \mathbf{20}k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} 20 & = & 2 \cdot 7 + 6 & 6 & = & 1 \cdot 20 - 2 \cdot 7 \\ 7 & = & 1 \cdot 6 + 1 & 1 & = & 7 - 1 \cdot 6 = 7 - 1 \cdot (1 \cdot 20 - 2 \cdot 7) \\ & & & & = & 3 \cdot 7 + (-1) \cdot 20 \end{array}$$

Also $e = 3$. (Allgemein $e = 3 + 20l$, $l \in \mathbb{Z}$)

Pia liest die Homepage von Frank und will ihm die Nachricht $\boxed{n = 6}$ übermitteln. Sie berechnet

Modulo 33: $n^v = 6^7 = 36^3 \cdot 6 \equiv 3^3 \cdot 6 = 27 \cdot 6 = 54 \cdot 3$
$\equiv 21 \cdot 3 = 63 \equiv 30 \mod 33$

und schickt Frank $\boxed{N = 30}$. Frank liest in Pias Mail $\boxed{N = 30}$ und berechnet

Modulo 33: $N^e = 30^3 \equiv (-3)^3 = -27 \equiv 6 \mod 33$

erhält also $\boxed{n = 6}$ zurück.

Datei: `Kryptographie73-RSA-Lueckentext`

Lösung: Ist bereits im Aufgabentext enthalten.

Mündlich: e muss zwischen 1 und $m-1$ liegen. Falls der erweiterte euklidische Algorithmus einen negativen Wert für e liefert, muss mit der allgemeinen Formel der richtige Wert für e ermittelt werden.

> **Anmerkung**
> In der letzten Aufgabe kann der Wert von e leicht erraten werden. Trotzdem sollte vorgeführt werden, wie man e systematisch berechnet.

> **Anmerkung**
> $\widetilde{m}$ ist keine Primzahl, deshalb muss man $e \cdot v \equiv 1 \mod \widetilde{m}$ von Hand lösen.

Aufgabe 7.5 (*Arbeitsblatt 7.5 (RSA-Verschlüsselung knacken), Aufgabe 4*)

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 55$ und $v = 7$. Er erhält von Peter die Zahl $N = 25$.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Datei: `Kryptographie74-RSA-55`

Lösung: $m = 55 = 5 \cdot 11 \Rightarrow p = 5$, $q = 11$, $\widetilde{m} = 4 \cdot 10 = 40$,

Berechne e mit $7e \equiv 1 \mod 40$, d.h. $\mathbf{7}e + \mathbf{40}k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} \mathbf{40} & = & 5 \cdot \mathbf{7} + 5 & 5 & = & 1 \cdot \mathbf{40} - 5 \cdot \mathbf{7} \\ \mathbf{7} & = & 1 \cdot 5 + 2 & 2 & = & \mathbf{7} - 1 \cdot 5 \\ 5 & = & 2 \cdot 2 + 1 & 1 & = & 5 - 2 \cdot 2 \;=\; 5 - 2 \cdot (\mathbf{7} - 1 \cdot 5) \;=\; 3 \cdot 5 - 2 \cdot \mathbf{7} \\ & & & & & = \; 3(1 \cdot \mathbf{40} - 5 \cdot \mathbf{7}) - 2 \cdot \mathbf{7} \;=\; 3 \cdot \mathbf{40} - 17 \cdot \mathbf{7} \end{array}$$

Damit wäre $e = -17$.

Das passt nicht, wir suchen eine Lösung von $7e \equiv 1 \mod 40$ mit $1 < e < 40$.

Mit $-17 \equiv 23 \mod 40$ folgt $e = 23$.

Damit:

$$\begin{aligned} N^e &= 25^{23} = 625^{11} \cdot 25 \equiv 20^{11} \cdot 25 = 400^5 \cdot 20 \cdot 25 \equiv 15^5 \cdot 500 \\ &\equiv 225^2 \cdot 15 \cdot 5 \equiv 5^2 \cdot 75 = 25 \cdot 20 = 500 \equiv 5 \mod 55, \end{aligned}$$

also $n = 5$. Probe:

$$n^v = 5^7 = 125^2 \cdot 5 \equiv 15^2 \cdot 5 \equiv 225 \cdot 5 \equiv 5 \cdot 5 = 25 = N \mod 55.$$

> **Anmerkung**
> Die folgende Zusatzaufgabe ist einfacher als die letzte Aufgabe. Hintergrund dieser Reihenfolge ist, dass die Schüler:innen ein Mal den euklidischen Algorithmus durchführen sollen. In der Zusatzaufgabe kann der Wert von e leicht erraten werden.

Aufgabe 7.6 (*Arbeitsblatt 7.5 (RSA-Verschlüsselung knacken), Aufgabe 5*)

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 51$ und $v = 3$. Er erhält von Jane die Zahl $N = 8$ als verschlüsselte Botschaft.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Datei: `Kryptographie75-RSA-51`

Lösung: $m = 51 = 3 \cdot 17 \Rightarrow p = 3,\ q = 17,\ \widetilde{m} = 2 \cdot 16 = 32.$

Berechne e mit mit $3e \equiv 1 \mod 32$, d.h. $\mathbf{3}e + \mathbf{32}k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} \mathbf{32} & = & 10 \cdot \mathbf{3} + 2 & 2 & = & 1 \cdot \mathbf{32} - 10 \cdot \mathbf{3} \\ \mathbf{3} & = & 1 \cdot 2 + 1 & 1 & = & \mathbf{3} - 1 \cdot 2 \ = \ \mathbf{3} - (1 \cdot \mathbf{32} - 10 \cdot \mathbf{3}) \ = \ 11 \cdot \mathbf{3} - 1 \cdot \mathbf{32} \end{array}$$

Also $e = 11$.

Damit folgt $N^e = 8^{11} = 64^5 \cdot 8 \equiv 13^5 \cdot 8 = 169^2 \cdot 13 \cdot 8 \equiv 16^2 \cdot 104 \equiv 1 \cdot 2 = 2 \mod 51$.

Also gilt $n = 2$. (Probe: $n^v = 2^3 = 8 = N$.)

Tafelanschrieb

10. RSA-Verschlüsselung

Seien $p, q, m, \widetilde{m}, e, v, n, N$ gemäß dem RSA-Algorithmus gewählt bzw. berechnet.

Wir beweisen, dass $\boxed{N^e \equiv n \mod m}$ gilt.

Kleiner Fermat: Ist p Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p, so gilt $a^{p-1} \equiv 1 \mod p$.

Vorbemerkung 1: $\underbrace{a \equiv n \mod p}_{a-n \text{ durch } p \text{ teilbar}}$ und $\underbrace{a \equiv n \mod q}_{a-n \text{ durch } q \text{ teilbar}} \overset{p,q \text{ Primzahlen}}{\Leftrightarrow} a \equiv n \mod \underbrace{pq}_{=m}$.

Vorbemerkung 2: $e \cdot v \equiv 1 \mod \widetilde{m}$
$\Leftrightarrow\ e \cdot v = 1 + k\widetilde{m} = 1 + k(p-1)(q-1)$ mit einem $k \in \mathbb{Z}$.

Wir rechnen zunächst nur modulo p.
Vorbemerkung 1 $\Rightarrow\ N^e \equiv (n^v)^e = n^{e \cdot v} \mod p$

Fall $\mathrm{ggT}(n, p) = 1$:

$$n^{e \cdot v} \overset{\text{Vorbemerkung 2}}{=} n^{1+k(p-1)(q-1)} = n \cdot (n^{p-1})^{k(q-1)} \overset{\substack{\text{kleiner} \\ \text{Fermat}}}{\equiv} n \cdot 1^{k(q-1)} = n \mod p$$

Fall $\mathrm{ggT}(n, p) = p$: Dann ist $n = l \cdot p$ und somit $n \equiv 0 \mod p$.
$\Rightarrow\ n^{e \cdot v} \equiv 0^{e \cdot v} = 0 \equiv n \mod p$.

In beiden Fällen gilt also

$$N^e \equiv n^{e \cdot v} \equiv n \mod p. \tag{1}$$

Nun rechnen wir nur modulo q. Indem man p und q vertauscht, folgt genauso, dass

$$N^e \equiv n^{e \cdot v} \equiv n \mod q \tag{2}$$

gilt.

(1) und (2) $\overset{\substack{\text{Vorbemerkung 1} \\ \Rightarrow \\ pq=m}}{}$ $\boxed{N^e \equiv n \mod m}$. $\square$

Vorgehen: Da der Beweis relativ lange ist, wurde zu Beginn das Ziel durch einen farbigen Kasten markiert. Dann signalisiert der selbe farbige Kasten am Schluss, dass das Ziel erreicht wurde.

Mündlich: Im Fall $\mathrm{ggT}(n,p) = p$ kann der kleine Fermat nicht angewandt werden.

> **Anmerkung**
> Durch die Kongruenzgleichung (1) erhält man den Wert von n nur bis auf Vielfache von p eindeutig. Das reicht nicht. Man braucht (2), damit die Lösung eindeutig modulo m ist.

8.6 Schriftliche Aufgaben (ohne Lösungen)

Aufgabe 7.7 (*Arbeitsblatt 7.6 (Schriftliche Aufgaben), Aufgabe 6*)

Gegeben ist die Kongruenzgleichung

$$21x \equiv a \mod 51, \tag{1}$$

wobei $a \in \mathbb{N}$ später gewählt wird.

a) Gib eine zu (1) äquivalente diophantische Gleichung an.

$\square$ mit $y \in \mathbb{Z}$. (2)

b) Welche Bedingung müssen a und $\mathrm{ggT}(21,51)$ erfüllen, damit die diophantische Gleichung (2) Lösungen besitzt?

Bedingung: $\square$.

c) Kreuze in der Tabelle an, für welche der gegebenen Zahlen a die Kongruenzgleichung (1) jeweils Lösungen besitzt.

$a =$	1	3	7	17	21	51
(1) besitzt Lösungen						

Datei: `Kryptographie790-Kongruenzgleichung`

Weiter auf nächster Seite

Aufgabe 7.8 (*Arbeitsblatt 7.6 (Schriftliche Aufgaben), Aufgabe 7*)

Gegeben ist die Kongruenzgleichung

$$e \cdot 7 \equiv 1 \mod 60. \tag{3}$$

a) Gib eine zu (3) äquivalente diophantische Gleichung an.

$\square$ mit $y \in \mathbb{Z}$. (4)

b) Berechne mit Hilfe des erweiterten euklidischen Algorithmus eine Lösung von (4).

Erweiterter euklidischer Algorithmus:

Eine Lösung von (4): $(e \mid y) =$ $\square$.

c) Gib alle ganzzahligen Lösungen von (4) an.

$(e \mid y) =$ $\square$ mit $k \in \mathbb{Z}$.

d) Gib alle Lösungen von (3) an. $e =$ $\square$.

e) Gib die einzige Lösung x von (3) an, für die $1 < x < 60$ gilt.

$e =$ $\square$.

f) Mache die Probe. $e \cdot 7 =$ $\square$ $=$ $\square$ $\cdot 60 + 1$.

Datei: `Kryptographie791-Kongruenzgleichung-konkret`

Aufgabe 7.9 (*Arbeitsblatt 7.6 (Schriftliche Aufgaben), Aufgabe 8*)

Noah möchte sich Nachrichten schicken lassen, die mit dem Elgamal-Verfahren verschlüsselt sind. Er wählt $p = 31$, $g = 11$, $e = 24$ und berechnet

$$\begin{aligned} [11]^2 &= [121 - 124] = [-3], \\ [11]^6 &= [-3]^3 = [-27] = [4], \\ [A] &= [11]^{24} = [4]^4 = [64] \cdot [4] = [2] \cdot [4] = [8] \text{ in } \mathbb{Z}_{31}. \end{aligned}$$

Er veröffentlich also auf seiner Homepage $p = 31$, $g = 11$ und $A = 8$.

a) Anna möchte die Nachricht $n = 10$ für Noah verschlüsseln. Sie wählt den Verschlüsselungsexponent $v = 4$ und berechnet in $\mathbb{Z}_{31}$

$[B] =$ ☐, $[A]^4 =$ ☐, $[N] =$ ☐.

b) Emilia schickt an Noah $B = 4$ und $N = 3$. Berechne

$[B]^{-e} =$ ☐, $[n] =$ ☐ in $\mathbb{Z}_{31}$.

Datei: `Kryptographie792-Elgamal`

Aufgabe 7.10 (*Arbeitsblatt 7.6 (Schriftliche Aufgaben), Aufgabe 9*)

Frank veröffentlicht auf seiner Homepage $m = 77$ und $v = 43$, damit Personen ihre Nachrichten an ihn mit RSA verschlüsseln können..

a) Gib die Werte an, die er gewählt bzw. berechnet hat.

$p =$ ☐, $q =$ ☐, $\widetilde{m} =$ ☐, $e =$ ☐ (beachte die vorigen Aufgaben).

b) Andrew schickt Frank die Zahl $N = 2$. Entschlüssle die Nachricht.

$n =$ ☐.

Datei: `Kryptographie793-RSA`

8.7 Hinweise und Ergänzungen

Hier noch eine Übersicht über Bezeichnungen für verschiedene Verschlüsselungsmethoden:

Definition: Eine Verschlüsselungsmethode, bei der mit dem selben Schlüssel ver- und entschlüsselt wird, heißt symmetrische Verschlüsselung. Z.B. Permutationsverschlüsselung, Vigenère.

Bei einer asymmetrischen Verschlüsselung werden zum Ver- und Entschlüsseln verschiedene Schlüssel verwendet, z.B. Diffie-Hellman-Merkle, RSA.

Hybride Verschlüsselung: Hier wird ein Schlüssel für eine symmetrische Verschlüsselung einmalig erzeugt (Session-key). Dann wird der Schlüssel mit einem asymmetrischen Verfahren übertragen, die Nachricht wird symmetrisch verschlüsselt übertragen.

9 Hinweise zum Erstellen von Aufgaben

9.1 Erstellen von Aufgaben zum euklidischen Algorithmus

Von unten nach oben rechnen. Dadurch kann der ggT, die Größe der Zahlen und die Anzahl der Zeilen kontrolliert werden.

Z.B. Vorgabe: 4 Zeilen und $\mathrm{ggT}(a,b) = 5$. Die rechten Seiten der Gleichungen werden zuerst eingetragen, dann wird die linke Seite ausgerechnet. In jeder Zeile kann der auf der rechten Seite der Faktor beliebig gewählt werden. Die wählbaren Faktoren sind farbig markiert.

$$\begin{aligned} 10 &= 2 \cdot 5 \\ 35 &= 3 \cdot 10 + 5 \\ 45 &= 1 \cdot 35 + 10 \\ 170 &= 3 \cdot 45 + 35 \end{aligned}$$

Zur Berechnung von $\mathrm{ggT}(170, 45) = 5$ werden im euklidischen Algorithmus die obigen Zeilen von unten nach oben durchlaufen.

9.2 Erstellen von Aufgaben zum erweiterten euklidischen Algorithmus

Zunächst eine Vorbemerkung: Es genügt, Aufgabenstellungen für $\mathrm{ggT}(a,b) = 1$ zu kreieren. Multipliziert man danach a, b mit derselben Zahl $s \in \mathbb{N}$, so besteht der euklidische Algorithmus für $\mathrm{ggT}(sa, sb) = s$ aus den selben Rechenschritten, es werden nur die Reste mit s multipliziert.

Nun zur Konstruktion einer Aufgabe für den erweiterten euklidischen Algorithmus mit 4 Zeilen, $\mathrm{ggT}(a,b) = 1$ und frei wählbare Werten für $k, l, n, m \in \mathbb{N}$. Auch hier wird der euklidische Algorithmus rückwärts durchgeführt.

$$\begin{array}{rcl|rcl} k &=& k \cdot 1 & & & \\ lk+1 &=& l \cdot k + 1 & 1 &=& (lk+1) - lk \\ lkm + m + k &=& m \cdot (lk+1) + k & k &=& b - m(lk+1) \\ \underbrace{lkmn + mn + mk + lk + 1}_{=:a} &=& n \cdot (\underbrace{lkm + m + k}_{=:b}) + lk + 1 & lk+1 &=& a - nb \end{array}$$

$$\begin{aligned} \Rightarrow\ \mathrm{ggT}(a,b) &= 1 = (lk+1) - lk = (lk+1) - l\big(b - m(lk+1)\big) \\ &= (1+lm)(lk+1) - l \cdot b = (1+lm)(a - n \cdot b) - l \cdot b \\ &= (1+lm) \cdot a - (n + lmn + l) \cdot b \end{aligned}$$

Man sieht, dass der Wert von k für die Darstellung des $\mathrm{ggT}(a,b)$ keine Rolle spielt. Will man nun die Faktoren in der Darstellung von $\mathrm{ggT}(a,b)$ vorgeben, so wählt man l, m, n entsprechend. Mit der Abkürzung $r := 1 + lm$ für den Faktor vor a können dann a, b durch

$$b = kr + m, \quad a = n \cdot b + lk + 1$$

einfacher berechnet werden. Für die Wahl von $k = 3,\ l = 5,\ m = 8,\ n = 1$ ergeben sich $a = 147$, $b = 131$ und

$$\mathrm{ggT}(147, 131) = 1 = 41 \cdot 147 - 46 \cdot 131.$$

Multiplikation mit 3 liefert

$$\mathrm{ggT}(441, 393) = 3 = 41 \cdot 441 - 46 \cdot 393.$$

10 Heftaufschrieb

Dieses Kapitel enthält die Teile des Skripts, die bei den Schüler:innnen im Aufschrieb stehen sollen. Dies dient unter anderem der Kontrolle, ob aus den vorbereiteten Tafelaufschrieben ein sinnvoller Heftaufschrieb entstehen kann.

Einheit 1

Zahlentheorie und Kryptographie

1. Diophantische Gleichungen

Gegeben:	$a, b, c \in \mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$
Gesucht:	$x, y \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
so dass	$ax + by = c$
Vereinbarung:	Schreibe die Lösungen als Zahlenpaare $(x \mid y)$

Hier wurde Arbeitsblatt 1.1 (Diophantische Gleichungen) ausgegeben.

Definition: 1) Seien $a \in \mathbb{Z}$, $k \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Dann heißt k Teiler von a, geschrieben $k \mid a$, falls es ein $a' \in \mathbb{Z}$ gibt, so dass $a = a' \cdot k$.

Beispiele: $a = 35$ hat die Teiler $1, 5, 7, 35$, denn
$a = 35 \cdot 1 \quad (a' = 35)$
$a = 7 \cdot 5 \quad (a' = 7)$
$a = 5 \cdot 7 \quad (a' = 5)$
$a = 1 \cdot 35 \quad (a' = 1)$

$a = -35$ hat die selben Teiler.

$a = 0$ hat alle positiven natürlichen Zahlen als Teiler: $\underbrace{0}_{a} = \underbrace{0}_{a'} \cdot k$.

2) Seien $a, b \in \mathbb{Z}$, nicht beide 0. Dann ist der größte gemeinsame Teiler von a, b definiert durch

$$\mathrm{ggT}(a, b) \;:=\; \max \underbrace{\{k \in \mathbb{N}_+ : k \mid a \text{ und } k \mid b\}}_{\text{Menge der gemeinsamen Teiler von } a \text{ and } b}.$$

Beispiel: $a = 70,\ b = 98$:

a hat die Teiler $1, 2, 5, 7, 10, 14, 35, 70$,
b hat die Teiler $1, 2, 7, 14, 49, 98$,
Menge der gemeinsamen Teiler: $\{1, 2, 7, 14\}$,
Größtes Element der Menge: $\mathrm{ggT}(70, 98) = 14$.

Satz: Aus $k \mid a$ und $k \mid b$ und $x, y \in \mathbb{Z}$ folgt $k \mid (ax + by)$.

Beweis:
$$\begin{aligned} & k \mid a \;\Rightarrow\; a = a'\,k \\ & k \mid b \;\Rightarrow\; b = b'\,k \\ \Rightarrow\;\; & ax + by \;=\; a'\,kx + b'\,ky \;=\; \underbrace{(a'\,x + b'\,y)}_{\in\mathbb{Z}}\,k \\ \Rightarrow\;\; & k \mid (ax + by) \qquad \square \end{aligned}$$

Satz: Besitzt die Gleichung $ax + by = c$ eine Lösung $(x \mid y)$ mit $x, y \in \mathbb{Z}$, so folgt $\mathrm{ggT}(a, b) \mid c$.

Beweis: $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$
$\overset{\text{letzter Satz}}{\Rightarrow}$ $\mathrm{ggT}(a, b) \mid \underbrace{(ax + by)}_{=c}$. $\square$

Folgerung: Ist $\mathrm{ggT}(a, b)$ kein Teiler von c, so hat $ax + by = c$ keine ganzzahlige Lösung.

Hier wurde Arbeitsblatt 1.2 (Diophantische Gleichungen und ggT) ausgegeben.

2. Der euklidische Algorithmus

Teilen mit Rest:

$13 : 4 = 3 \text{ R } 1$ bedeutet: $13 = 3 \cdot 4 + 1$

$223 : 25 = 8 \text{ R } 23$ bedeutet: $223 = 8 \cdot 25 + 23$

Satz (Teilen mit Rest): Seien $a, b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{N} = \{0, 1, \ldots\}$, so dass gilt:

$$a = kb + r \quad \text{und} \quad 0 \leq r \leq b - 1.$$

Anmerkung: Ohne die Bedingung $0 \leq r \leq b - 1$ sind k, r nicht eindeutig, z.B.

$$23 = 4 \cdot 5 + 3 \quad \text{und} \quad 23 = 3 \cdot 5 + 8.$$

Hier wurde Arbeitsblatt 1.3 (Teilen mit Rest) ausgegeben.

Euklidischer Algorithmus: Gesucht $\mathrm{ggT}(468, 60)$.

Teilen mit Rest:

$$\begin{aligned} 468 &= 7 \cdot 60 + 48 \\ 60 &= 1 \cdot 48 + 12 \\ 48 &= 4 \cdot 12 \end{aligned} \qquad \Rightarrow \ \mathrm{ggT}(468, 60) = 12$$

Stimmt das immer?

Satz: Sei $a = k \cdot b + r$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Beweis: 1) $\mathrm{ggT}(b, r)$ teilt b und r.

$\overset{\text{früherer Satz}}{\Rightarrow}$ $\mathrm{ggT}(b, r)$ teilt $a = k \cdot b + 1 \cdot r$

$\Rightarrow$ $\mathrm{ggT}(b, r)$ teilt a und b

$\Rightarrow$ $\mathrm{ggT}(b, r) \leq \mathrm{ggT}(a, b)$.

2) Löse die Gleichung nach r auf: $r = a - k \cdot b$.

Wie vorher folgt: $\mathrm{ggT}(a, b)$ teilt b und r

$\Rightarrow$ $\mathrm{ggT}(a, b) \leq \mathrm{ggT}(b, r)$.

1) und 2) $\Rightarrow$ $\mathrm{ggT}(b, r) = \mathrm{ggT}(a, b)$. $\square$

Euklidischer Algorithmus für $\mathrm{ggT}(98, 126)$:

$$\begin{array}{rcl} \overset{a}{126} &=& 1 \cdot \overset{b}{98} + \overset{r}{28} \\ 98 &=& 3 \cdot 28 + 14 \\ 28 &=& 2 \cdot 14 \end{array} \quad \begin{array}{c} \overset{\text{Satz}}{\Rightarrow} \\ \Rightarrow \\ \Rightarrow \end{array} \quad \begin{array}{rcl} \mathrm{ggT}(\overset{a}{126}, \overset{b}{98}) &=& \mathrm{ggT}(\overset{b}{98}, \overset{r}{28}) \\ \mathrm{ggT}(98, 28) &=& \mathrm{ggT}(28, 14) \\ \mathrm{ggT}(28, 14) &=& 14 \\ \hline \Rightarrow \ \mathrm{ggT}(126, 98) &=& 14 \end{array}$$

Hier wurde Arbeitsblatt 1.4 (Euklidischer Algorithmus) ausgegeben.

Einheit 2

3. Eine Lösung berechnen

Gesucht: Alle ganzzahligen Lösungen von $110x + 32y = 8$.

Satz: Zu beliebig gewählten natürlichen Zahlen a, b gibt es ganze Zahlen x, y, so dass

$$ax + by \;=\; \mathrm{ggT}(a, b).$$

Beispiel: Erweiterter Euklidischer Algorithmus für $110x + 32y \;=\; \mathrm{ggT}(110, 32)$.

Schritt 1:	Schritt 2:
$110 = 3 \cdot 32 + 14$	$14 = 110 - 3 \cdot 32$
$32 = 2 \cdot 14 + 4$	$4 = 32 - 2 \cdot 14$
$14 = 3 \cdot 4 + 2$	$2 = 14 - 3 \cdot 4$
$4 = 2 \cdot 2$	

$$\begin{aligned}
\Rightarrow\; \mathrm{ggT}(110, 32) \;=\; 2 &= 14 - 3(\overbrace{32 - 2 \cdot 14}^{4=}) \\
&= 14 - 3 \cdot 32 + 6 \cdot 14 \;=\; 7 \cdot 14 - 3 \cdot 32 \\
&= 7(\overbrace{110 - 3 \cdot 32}^{14=}) - 3 \cdot 32 \;=\; 7 \cdot 110 - 21 \cdot 32 - 3 \cdot 32 \\
&= 7 \cdot 110 - 24 \cdot 32
\end{aligned}$$

$\Rightarrow\; (x \mid y) = (7 \mid -24)$ ist eine Lösung.

Hier wurde Arbeitsblatt 2.1 (Eine Lösung berechnen) ausgegeben.

Satz: Seien $a, b, c \in \mathbb{N}$ gegeben, so dass $\mathrm{ggT}(a, b) \mid c$. Dann hat

$$ax + by \;=\; c \;(= n \cdot \mathrm{ggT}(a, b))$$

mindestens eine ganzzahlige Lösung $(x \mid y)$.

Beweis: Es gibt ein $n \in \mathbb{N}$, so dass $c = n \cdot \mathrm{ggT}(a, b)$.

Letzter Satz $\Rightarrow$ es gibt ganzzahlige x, y mit

$ax + by \;=\; \mathrm{ggT}(a, b) \qquad \mid \cdot n$

$\Leftrightarrow\; n(ax + by) \;=\; n \cdot \mathrm{ggT}(a, b)$

$\Leftrightarrow\; a(nx) + b(ny) \;=\; c$

$\Rightarrow\; (nx \mid ny)$ ist ganzzahlige Lösung. $\square$

Beispiel: $110x + 32y = \mathrm{ggT}(110, 32) = 2$ hat die Lösung $(7 \mid -24)$.

$\Rightarrow\; 110x + 32y = 8 = 4 \cdot 2$ hat die Lösung $(4 \cdot 7 \mid 4 \cdot (-24)) = (28 \mid -96)$.

Hier wurde Arbeitsblatt 2.2 (Mehrere Lösungen finden) ausgegeben.

4. Alle Lösungen berechnen

Beobachtung: Die Gleichung $3x + 2y = 1$ hat die Lösungen

		$+2$	$+2$	$+2$	$+2$
x	-1	1	3	5	$\ldots$
y	2	-1	-4	-7	$\ldots$
		-3	-3	-3	-3

D.h. x wird in 2er Schritten erhöht und y in 3er Schritten erniedrigt.

Satz: 1) Ist $(x_0 \mid y_0)$ eine Lösung von $ax + by = c$, dann sind alle Zahlenpaare

$$(x \mid y) \;=\; (x_0 + k \cdot b \mid y_0 - k \cdot a) \text{ mit } k \in \mathbb{Z} \qquad (*)$$

ebenfalls Lösungen.

2) Gilt $\mathrm{ggT}(a, b) = 1$, dann sind durch $(*)$ alle Lösungen gegeben.

Beweis: 1) Durch $(*)$ sind Lösungen gegeben, denn

$ax + by \;=\; a(x_0 + kb) + b(y_0 - ka) \;=\; ax_0 + \cancel{akb} + by_0 - \cancel{bka} \;=\; c.$

2) Sei $(x \mid y)$ irgendeine Lösung von $ax + by = c$.

Es gilt $a(x - x_0) + b(y - y_0) \;=\; ax + by - (ax_0 + by_0) \;=\; c - c \;=\; 0$

$\Rightarrow\; b(y - y_0) \;=\; -a(x - x_0).$

$\mathrm{ggT}(a, b) = 1 \;\Rightarrow\; b \mid (x - x_0) \;\Rightarrow\; x - x_0 = k \cdot b$ mit geeignetem $k \in \mathbb{Z}$.

$\Rightarrow\; y - y_0 \;=\; -\frac{a}{b}(x - x_0) \;=\; -\frac{a}{b} \cdot k \cdot b \;=\; -k \cdot a.$

$\Rightarrow\; y \;=\; y_0 - k \cdot a, \quad x \;=\; x_0 + k \cdot b$

$\Rightarrow\; (x \mid y)$ wird durch die Formel $(*)$ beschrieben. $\square$

Beispiel: $$110\,x + 32\,y = 8 \qquad (1)$$

hat die Lösung $(x_0 \mid y_0) = (28 \mid -96)$.

1) des Satzes: $(x \mid y) = (28 - k \cdot 32 \mid -96 + k \cdot 110)$ mit $k \in \mathbb{Z}$ sind Lösungen.

Teile die Gleichung (1) auf beiden Seiten durch $2 = \mathrm{ggT}(110, 32)$:

$$55\,x + 16\,y \;=\; 4 \qquad (2)$$

hat die selben Lösungen wie (1), und $\mathrm{ggT}(55, 16) = 1$.

2) des Satzes: Alle Lösungen von (2) sind

$$(x \mid y) = (28 + k \cdot 16 \mid -96 - k \cdot 55) \text{ mit } k \in \mathbb{Z}.$$

Dies sind auch alle Lösungen von (1).

Hier wurde Arbeitsblatt 2.3 (Alle Lösungen bestimmen) ausgegeben.

Einheit 3

Hier wurde Arbeitsblatt 3.1 (Teilen durch 9) ausgegeben.

5. Kongruenzen

Definition: Seien a, b ganze Zahlen, $m \in \mathbb{N}_+ = \{1, 2, \ldots\}$. Schreibe

$$a \equiv b \mod m \qquad (a \text{ ist kongruent zu } b \text{ modulo } m),$$

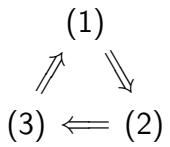
falls $a - b$ durch m teilbar ist.

Beispiel: $15 \equiv 3 \mod 6$, denn $15 - 3 = 12$ ist durch 6 teilbar.

Satz (Kongruenzkriterien): Folgende Aussagen sind äquivalent:

(1) $a \equiv b \mod m$
(2) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$
(3) a und b lassen beim Teilen durch m den selben Rest.

Beweisprinzip Ringschluss:



Beweis: (1) ⇒ (2):

$$\begin{aligned} a \equiv b \mod m &\Leftrightarrow m \mid (a-b) \\ &\Rightarrow \text{Es gibt ein } k \in \mathbb{Z}, \text{ so dass } a-b = k \cdot m \quad \big| +b \\ &\Rightarrow a = km + b = b + km \end{aligned}$$

(2) ⇒ (3): Sei r der Rest beim Teilen von b durch m,
d.h. $b = lm + r$ mit einem $l \in \mathbb{Z}$.

$$\begin{aligned} (2) \Rightarrow a &= b + km \\ &= lm + r + km \\ &= \underbrace{(l+k)}_{\in\mathbb{Z}} m + r \end{aligned}$$

$\Rightarrow$ a lässt beim Teilen durch m den selben Rest r wie b.

(3) ⇒ (1): $a = km + r,\ b = lm + r$ mit $k, l \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow a - b &= km + r - (lm + r) \\ &= km + \cancel{r} - kl - \cancel{r} \\ &= (k-l)m \\ \Rightarrow m &\mid (a-b) \\ \Leftrightarrow a &\equiv b \mod m \end{aligned}$$

□

Aus Aufgabe 1: b) $2005 : 9 = 222$ R 7
$\Leftrightarrow 2005 = 9 \cdot 222 + 7$
$\Rightarrow 2005 \equiv 7 \mod 9$

c) $2050 \equiv 7 \mod 9$
$\Rightarrow 2050 \equiv 2005 \mod 9$

Hier wurde Arbeitsblatt 3.2 (Kongruenzgleichungen) ausgegeben.

Satz (Rechenregeln für Kongruenzen):

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann:

$$\begin{aligned} &a_1) && -a \equiv -b && \mod m \\ &a_2) && a + c \equiv b + d && \mod m \\ &a_3) && ac \equiv bd && \mod m \\ &a_4) && a^2 \equiv b^2 && \mod m, \quad a^3 \equiv b^3 \mod m, \quad \ldots \end{aligned}$$

b) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann

$$\begin{aligned} &b_1) && a \equiv a && \mod m \\ &b_2) && b \equiv a && \mod m \\ &b_3) && a \equiv c && \mod m \end{aligned}$$

Beweis von a_3): Wir wissen $a = b + km$, $c = d + lm$ mit $k, l \in \mathbb{Z}$.
Wir suchen ein $j \in \mathbb{Z}$, so dass $ac = bd + jm$.

$$\begin{aligned} ac &= (b+km)(d+lm) \\ &= bd + blm + kmd + kmlm \\ &= bd + \underbrace{(bl + kd + klm)}_{\in\mathbb{Z}} m \\ \Rightarrow\ ac &= bd + jm \\ \Rightarrow\ ac &\equiv bd \mod m \end{aligned}$$ □

Hier wurde Arbeitsblatt 3.3 (Rechenregeln für Kongruenzen) ausgegeben.

Satz (Quersummenregel): Wir schreiben $Q(a)$ für die Quersumme einer natürlichen Zahl a. Wir bilden so lange die Quersummen $Q(a)$, $Q(Q(a)), \ldots$, bis sich eine Zahl b zwischen 1 und 9 ergibt. Dann gilt $a \equiv b \mod 9$.
Wenn $b = 9$, dann ist a durch 9 teilbar.

Beispiel: $a = 123456$: $Q(a) = 21$, $Q(Q(a)) = 3 \Rightarrow 123456 \equiv 3 \mod 9$

Beweis 1) $a \equiv Q(a) \mod 9$:

Eine natürliche Zahl a mit $n+1$ Stellen können wir darstellen als

$$a = \boxed{a_n}\boxed{a_{n-1}} \ldots \begin{array}{|c|c|c|}\hline a_2 & a_1 & a_0 \\ \hline \text{H} & \text{Z} & \text{E} \\ \hline \end{array} \Rightarrow a = \underbrace{a_0 \cdot 1}_{\equiv a_0} + \underbrace{a_1 \cdot 10}_{\equiv a_1} + \underbrace{a_2 \cdot 100}_{\equiv a_2} + \ldots + \underbrace{a_n \cdot 10^n}_{\equiv a_n \mod 9}.$$

$$\begin{array}{rcl} 10 &\equiv& 1 \mod 9 \\ \overset{\text{Satz a4)}}{\Rightarrow}\ 10^2 &\equiv& 1^2 \mod 9 \\ \vdots & & \\ 10^n &\equiv& 1 \mod 9 \end{array} \quad \overset{\text{Satz a3)}}{\Rightarrow} \quad \begin{array}{rcl} a_1 \cdot 10 &\equiv& a_1 \cdot 1 \mod 9 \\ a_2 \cdot 10^2 &\equiv& a_2 \cdot 1 \mod 9 \\ \vdots & & \\ a_n \cdot 10^n &\equiv& a_n \cdot 1 \mod 9 \end{array}$$

$$\overset{\text{Satz a2)}}{\Rightarrow}\ a \equiv \underbrace{a_0 + a_1 + a_2 + \ldots + a_n}_{=Q(a)} \mod 9.$$

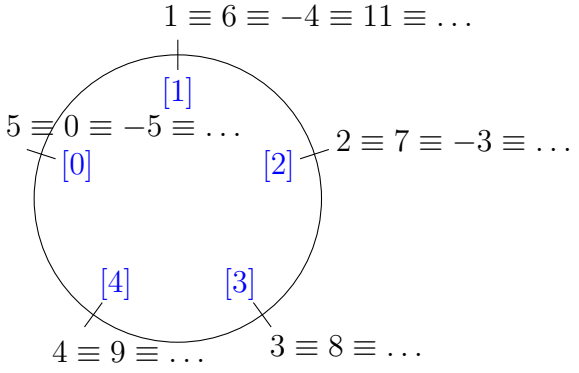
2) $a \equiv Q(a)$, $Q(a) \equiv Q(Q(a)) \overset{\text{Satz b3)}}{\Rightarrow} a \equiv Q(Q(a)) \Rightarrow a \equiv Q(Q(Q(a))) \ldots$ □

Hier wurde Arbeitsblatt 3.4 (Die Quersummenregel) ausgegeben.

Einheit 4

6. Rechnen mit Restklassen

Der Zahlenring modulo 5:



Betrachte alle Zahlen, die beim Teilen durch eine Zahl $m \in \mathbb{N}_+$ den selben Rest lassen. Diese Zahlen werden zu einer Menge zusammengefasst, der Restklasse.

Definition: Die Restklasse $[a]$ von a modulo m ist definiert durch

$$[a] := \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

a heißt Repräsentant der Restklasse $[a]$.

Beispiele modulo 5:

$$\begin{array}{llllllll} [0] & = & \{\ldots,-10,-5,0,5,10,\ldots\} & = & [5] & = & \ldots \\ [1] & = & \{\ldots,-9,-4,1,6,11,\ldots\} & = & [6] & = & [-4] & = & \ldots \\ [2] & = & \ldots \\ [3] & = & \ldots & = & [8] & = & \ldots \\ [4] & = & \ldots \end{array}$$

0 und 5 sind verschiedene Repräsentanten von $[0]$.

Definition: Die Menge aller Restklassen modulo m heißt Restklassenring modulo m, schreibe $\mathbb{Z}_m$.

Beispiel: $\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$.

Hier wurde Arbeitsblatt 4.1 (Restklassen) ausgegeben.

Definition: Für $a, b \in \mathbb{Z}$ definiert man

$$\begin{array}{rcl} [a]+[b] & := & [a+b] \\ [a]\cdot[b] & := & [ab] \end{array}$$

Beispiele modulo 5:

$$\begin{array}{rcl} [2]+[2] & = & [4] \\ [3]+[4] & = & [7] = [2] \\ [3]\cdot[4] & = & [12] = [2] \\ [-2]\cdot[-1] & = & [2] \\ [8]\cdot[9] & = & [72] = [2] \end{array}$$

Satz: Ist $[a] = [a']$ und $[b] = [b']$, so gilt $[a \cdot b] = [a' \cdot b']$ und $[a+b] = [a'+b']$.

Beweis: Ist $[a] = [a']$ und $[b] = [b']$, so folgt:

$$\begin{array}{ll} & a \equiv a' \mod m \quad \text{und} \quad b \equiv b' \mod m \\ \overset{\text{Rechenregeln für Kongruenzen}}{\Rightarrow} & ab \equiv a'b' \mod m \quad \text{und} \quad a+b \equiv a'+b' \mod m \\ \Rightarrow & [ab] = [a'b'] \quad \text{und} \quad [a+b] = [a'+b'] \end{array}$$ □

Hier wurde Arbeitsblatt 4.2 (Rechnen mit Restklassen) ausgegeben.

Satz: für $a, b \in \mathbb{Z}$ gilt $[a] - [b] = [a-b]$.

Beweis: $[a-b] + [b] = [a-b+b] = [a] \Rightarrow [a-b] = [a] - [b]$.

Beispiel zur Division: Was ist $\frac{[1]}{[2]}$ in $\mathbb{Z}_5$?

$$\frac{[1]}{[2]} = [x] \Leftrightarrow [2]\cdot[x] = [1]$$

Multiplikationstabelle in $\mathbb{Z}_5 \Rightarrow [x] = [3]$

Genauso: $\frac{[2]}{[3]} = [4]$, da $[3]\cdot[4] = [2]$.

Hier wurde Arbeitsblatt 4.3 (Differenzen und Quotienten von Restklassen) ausgegeben.

Existenz von Brüchen in $\mathbb{Z}_m$: Sei $m \in \mathbb{N}_+$, $a \in \{0, 1, \ldots, m-1\}$ und $b \in \{1, 2, \ldots, m-1\}$.

$$\begin{aligned} \frac{[a]}{[b]} = [x] &\Leftrightarrow [a] = [b] \cdot [x] = [bx] \\ &\Leftrightarrow a \equiv bx \mod m \\ &\Leftrightarrow a - bx = km \quad \text{für ein } k \in \mathbb{Z} \\ &\Leftrightarrow a = b\underbrace{x}_{\text{gesucht}} + m\underbrace{k}_{\text{unbekannt}} \end{aligned}$$

Dies ist eine diophantische Gleichung für die Unbekannten $x, k \in \mathbb{Z}$.

Wir wissen: Falls ggT$(b, m) \mid a$, ist die Gleichung lösbar.

Sei nun m eine Primzahl. Dann gilt ggT$(b, m) = 1$.

$\Rightarrow$ Für jedes $a \in \mathbb{N}$ existiert eine Lösung $(x_0 \mid k_0)$. Alle Lösungen sind durch

$$(x \mid k) = (x_0 + lm \mid k - lb) \text{ mit } l \in \mathbb{Z}$$

gegeben. Wir suchen nur $x = x_0 + lm$ und sehen $[x] = [x_0]$. Also ist $[x]$ eindeutig.

Damit ist bewiesen:

Satz vom Dividieren: Ist p eine Primzahl, und sind $a \in \{0, 1, \ldots, p-1\}$, $b \in \{1, \ldots, p-1\}$, so besitzt die Gleichung

$$[b] \cdot [x] = [a] \qquad \text{in } \mathbb{Z}_p$$

genau eine Lösung $[x]$, d.h. $\frac{[a]}{[b]} := [x]$ ist definiert.

Hier wurde Arbeitsblatt 4.4 (Quotienten von Restklassen) bearbeitet werden.

Einheit 5

... fand am Computer statt, es gibt keinen Aufschrieb.

Einheit 6

Zur Wiederholung wurde hier Arbeitsblatt 6.1 (Potenzen in $\mathbb{Z}_7$) ausgegeben.

7. Potenzen im Restklassenring

Kleiner Satz von Fermat: Sei p Primzahl, $a \in \mathbb{Z}$ kein Vielfaches von p. Dann gilt

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}_p \qquad \text{bzw.} \qquad a^{p-1} \equiv 1 \mod p.$$

Beispiel: $2^{40} \equiv ? \mod 19$:
Kleiner Fermat: $2^{19-1} \equiv 1 \mod 19$
$\Rightarrow 2^{40} = 2^{18} \cdot 2^{18} \cdot 2^4 \equiv 1 \cdot 1 \cdot 16 = 16 \mod 19$

Beweis: Wir untersuchen die Teilmenge
$A = \{[0a], [1a], [2a], \ldots, [(p-1)a]\}$
von $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$.

Schritt 1: Wir beweisen, dass alle p Restklassen $[0a]$, $[1a]$, $[2a]$, …, $[(p-1)a]$ verschieden sind.

Annahme: $[ja] = [ka]$ für zwei dieser Restklassen mit $j < k$. Dann folgt

$[0] = [ka] - [ja] = [ka - ja] = \big[(k-j)a\big] = [k-j] \cdot [a]$ mit $[k-j] \neq [0]$

$\overset{\text{Satz vom Dividieren}}{\Rightarrow}$ $[a] = [0]$, d.h. a ist Vielfaches von p $\Rightarrow$ Widerspruch

Also muss $[ja] \neq [ka]$ für $j \neq k$ gelten.

Schritt 2: Die Menge A hat p verschiedene Elemente und ist Teilmenge der p-elementigen Menge $\mathbb{Z}_p$. Also sind die Mengen gleich.

Schritt 3: Es ist klar, das $[0a] = [0]$ gilt. Wir entfernen nun dieses Element aus beiden Mengen. Das Produkt der restlichen Elemente muss gleich sein:

$$\begin{aligned} & [a] \cdot [2a] \cdot [3a] \cdots [(p-1)a] &&= [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \overset{\text{Satz vom Dividieren}}{\Leftrightarrow} \quad & [1] \cdot [2] \cdot [3] \cdots [p-1] \cdot [a]^{p-1} &&= [1] \cdot [2] \cdot [3] \cdots [p-1] \\ \overset{\text{Satz vom Dividieren}}{\Rightarrow} \quad & [a]^{p-1} = [1] \text{ in } \mathbb{Z}_p. \end{aligned}$$

□

Satz (Brüche berechnen): Sei p eine Primzahl und $[a] \in \mathbb{Z}_p$, $[a] \neq [0]$. Dann gelten:

1) $\dfrac{[1]}{[a]} \overset{\text{Kleiner Fermat}}{=} \dfrac{[a]^{p-1}}{[a]} = [a]^{p-2}$,

2) $\dfrac{[1]}{[a]^k} = \dfrac{[a]^{p-1}}{[a]^k} = [a]^{p-1-k}$ für $k = 1, 2, \ldots, p-2$.

Brüche können also durch Potenzen berechnet werden.

Hier wurde Arbeitsblatt 6.2 (Brüche berechnen) ausgegeben.

Definition: Ein Element $[g] \in \mathbb{Z}_m$ heißt Primitivwurzel, falls durch $[g]^k$ alle Elemente von $\mathbb{Z}_m$ außer $[0]$ dargestellt werden können.

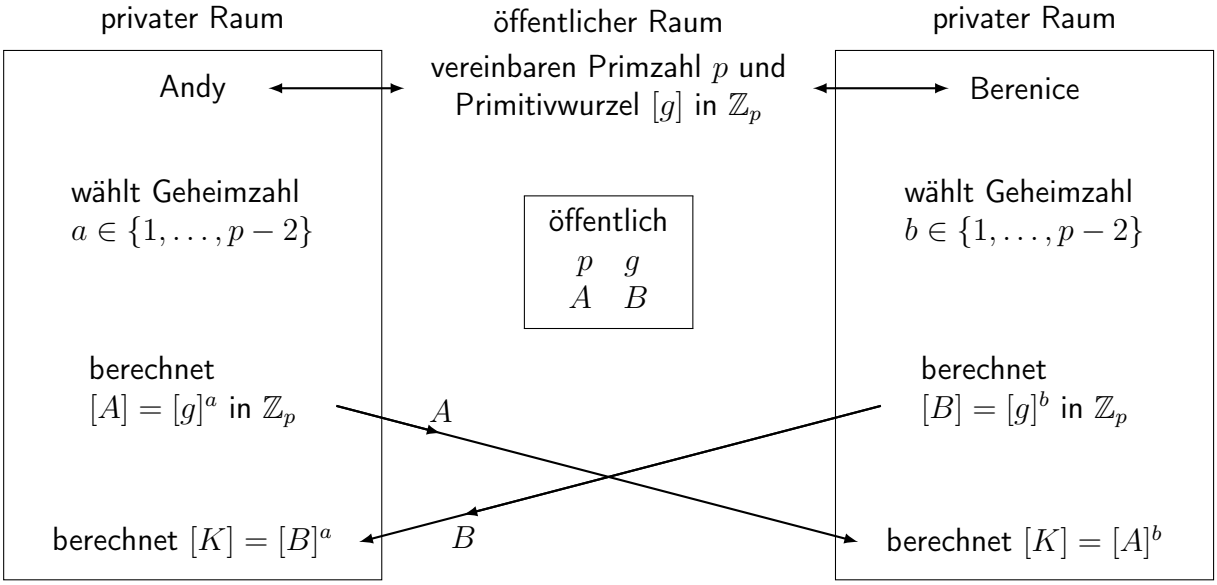
Beispiel: In $\mathbb{Z}_5$:

$k =$	1	2	3	4
$[2]^k =$	[2]	[4]	[3]	[1]
$[4]^k =$	[4]	[1]		

$\Rightarrow$ [2] ist eine Primitivwurzel, aber [4] nicht.

Hier wurde Arbeitsblatt 6.3 (Primitivwurzeln) ausgegeben.

8. Diffie-Hellman-Merkle-Schlüsselaustausch



Andy und Berenice erhalten die selbe Schlüsselzahl K, denn es gilt

$[B]^a = \left([g]^b\right)^a = [g]^{ab} = \left([g]^a\right)^b = [A]^b$.

Hier wurde Arbeitsblatt 6.4 (Schlüsselaustausch) ausgegeben.

Einheit 7

Zur Wiederholung wurde hier Arbeitsblatt 7.1 (Potenzen und kleiner Satz von Fermat) ausgegeben.

Hier wurde Arbeitsblatt 7.2 (Prinzip der Elgamal-Verschlüsselung) ausgegeben.

Hier wurde Arbeitsblatt 7.3 (Elgamal-Verschlüsselung) ausgegeben.

9. Kongruenzgleichungen

Beispiel: $x \cdot 9 \equiv 1 \mod 16$ $\quad (*)$

Lösung: $(*) \Leftrightarrow 9x + 16y = 1$ für ein $y \in \mathbb{Z}$.

Verallgemeinerter euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} 16 &=& 1\cdot 9 + 7 & \textcircled{7} &=& 16 - 1\cdot 9 \\ 9 &=& 1\cdot 7 + 2 & \textcircled{2} &=& 9 - 1\cdot 7 \\ 7 &=& 3\cdot 2 + 1 & 1 &=& 7 - 3\cdot\textcircled{2} = 7 - 3(9 - 1\cdot 7) \\ & & & &=& 4\cdot\textcircled{7} - 3\cdot 9 = 4(16 - 1\cdot 9) - 3\cdot 9 \\ & & & &=& 4\cdot 16 - 7\cdot 9 \end{array}$$

$\Rightarrow$ $(x, y) = (-7 \mid 4)$ ist eine Lösung.

Alle Lösungen: $(x, y) = (-7 + 16k \mid 4 - 9k)$ mit $k \in \mathbb{Z}$.

$\Rightarrow$ Alle Lösungen von $(*)$: $x = -7 + 16k$ mit $k \in \mathbb{Z}$.

Hier wurde Arbeitsblatt 7.4 (Das RSA-Verfahren) ausgegeben.

Hier wurde Arbeitsblatt 7.5 (RSA-Verschlüsselung knacken) ausgegeben.

10. RSA-Verschlüsselung

Seien $p, q, m, \widetilde{m}, e, v, n, N$ gemäß dem RSA-Algorithmus gewählt bzw. berechnet.

Wir beweisen, dass $\boxed{N^e \equiv n \mod m}$ gilt.

Kleiner Fermat: Ist p Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p, so gilt $a^{p-1} \equiv 1 \mod p$.

Vorbemerkung 1: $\underbrace{a \equiv n \mod p}_{a-n \text{ durch } p \text{ teilbar}}$ und $\underbrace{a \equiv n \mod q}_{a-n \text{ durch } q \text{ teilbar}} \overset{p,q \text{ Primzahlen}}{\Leftrightarrow} a \equiv n \mod \underbrace{pq}_{=m}$.

Vorbemerkung 2: $e \cdot v \equiv 1 \mod \widetilde{m}$
$\Leftrightarrow e \cdot v = 1 + k\widetilde{m} = 1 + k(p-1)(q-1)$ mit einem $k \in \mathbb{Z}$.

Wir rechnen zunächst nur modulo p.
Vorbemerkung 1 $\Rightarrow N^e \equiv (n^v)^e = n^{e\cdot v} \mod p$

Fall $\mathrm{ggT}(n, p) = 1$:

$$n^{e\cdot v} \overset{\text{Vorbemerkung 2}}{=} n^{1+k(p-1)(q-1)} = n \cdot (n^{p-1})^{k(q-1)} \overset{\text{kleiner Fermat}}{\equiv} n \cdot 1^{k(q-1)} = n \mod p$$

Fall $\mathrm{ggT}(n,p) = p$: Dann ist $n = l \cdot p$ und somit $n \equiv 0 \mod p$.

$\Rightarrow\ n^{e \cdot v} \equiv 0^{e \cdot v} = 0 \equiv n \mod p.$

In beiden Fällen gilt also

$$N^e \equiv n^{e \cdot v} \equiv n \mod p. \tag{1}$$

Nun rechnen wir nur modulo q. Indem man p und q vertauscht, folgt genauso, dass

$$N^e \equiv n^{e \cdot v} \equiv n \mod q \tag{2}$$

gilt.

(1) und (2) $\overset{\text{Vorbemerkung 1}}{\underset{pq=m}{\Rightarrow}}$ $\boxed{N^e \equiv n \mod m}$. $\square$

11 Ausarbeitung Unterrichtsstunde 1: Der euklidische Algorithmus

11.1 Stundenverlauf

Zeit	Unterrichtsschritte bzw. Unterrichtsarrangement	Sozialform L-S-Tätigkeit Methode	Was ich brauche
17:00	Erklärung, was eine (lineare) diophantische Gleichung ist	Tafelvortrag	
17:05	Entdeckungsphase, Ergebnisse an Tafel	Einzel-/ Partnerarbeit	Arbeitsblatt 1.1
17:18	Definition ggT	Tafelvortrag Beispiele fragend-entwickelnd	
17:30	Lösungskriterium	Tafelvortrag	
17:40	Anwendung	Einzel-/ Partnerarbeit	Arbeitsblatt 1.2
17:50	Teilen mit Rest	Tafelvortrag	
17:57	Übungsphase: Teil a) von allen, Teile b)-d) von verschiedenen Schüler:innen lösen lassen	Einzel-/ Partnerarbeit	Arbeitsblatt 1.3
18:05	Euklidischer Algorithmus	Tafelvortrag	
18:10	Begründung des euklidischen Algorithmus	Tafelvortrag	
18:20	Übungsphase, Ergebniskontrolle beim Durchgehen	Einzel-/ Partnerarbeit	Arbeitsblatt 1.4
18.30	Verabschiedung		

Kommentar: Stunde ist sehr voll und gerade so machbar.

11.2 Tafelanschriebe

Zahlentheorie und Kryptographie

1. Diophantische Gleichungen

Gegeben:	$a, b, c \in \mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$
Gesucht:	$x, y \in \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$
so dass	$ax + by = c$
Vereinbarung:	Schreibe die Lösungen als Zahlenpaare $(x \mid y)$

Arbeitsblatt 1.1: Diophantische Gleichungen (Besprechung an Tafel durch Zuruf)

Definition: 1) Seien $a \in \mathbb{Z}$, $k \in \mathbb{N}_+ = \{1, 2, 3, \ldots\}$. Dann heißt k Teiler von a, geschrieben $k \mid a$, falls es ein $a' \in \mathbb{Z}$ gibt, so dass $a = a' \cdot k$.

Beispiele: $a = 35$ hat die Teiler $1, 5, 7, 35$, denn
$a = 35 \cdot 1 \quad (a' = 35)$
$a = 7 \cdot 5 \quad (a' = 7)$
$a = 5 \cdot 7 \quad (a' = 5)$
$a = 1 \cdot 35 \quad (a' = 1)$

$a = -35$ hat die selben Teiler.

$a = 0$ hat alle positiven natürlichen Zahlen als Teiler: $\underbrace{0}_{a} = \underbrace{0}_{a'} \cdot k$.

2) Seien $a, b \in \mathbb{Z}$, nicht beide 0. Dann ist der größte gemeinsame Teiler von a, b definiert durch

$$\mathrm{ggT}(a, b) := \max \underbrace{\{k \in \mathbb{N}_+ : k \mid a \text{ und } k \mid b\}}_{\text{Menge der gemeinsamen Teiler von } a \text{ and } b}.$$

Beispiel: $a = 70,\ b = 98$:

a hat die Teiler $1, 2, 5, 7, 10, 14, 35, 70$,
b hat die Teiler $1, 2, 7, 14, 49, 98$,
Menge der gemeinsamen Teiler: $\{1, 2, 7, 14\}$,
Größtes Element der Menge: $\mathrm{ggT}(70, 98) = 14$.

Satz: Aus $k \mid a$ und $k \mid b$ und $x, y \in \mathbb{Z}$ folgt $k \mid (ax + by)$.

Beweis:
$$\begin{aligned} & k \mid a \ \Rightarrow\ a = a'k \\ & k \mid b \ \Rightarrow\ b = b'k \\ \Rightarrow\ & ax + by = a'kx + b'ky = \underbrace{(a'x + b'y)}_{\in\mathbb{Z}} k \\ \Rightarrow\ & k \mid (ax + by) \qquad \square \end{aligned}$$

Satz: Besitzt die Gleichung $ax + by = c$ eine Lösung $(x \mid y)$ mit $x, y \in \mathbb{Z}$, so folgt $\mathrm{ggT}(a, b) \mid c$.

Beweis: $\mathrm{ggT}(a, b) \mid a$ und $\mathrm{ggT}(a, b) \mid b$
$\overset{\text{letzter Satz}}{\Rightarrow}$ $\mathrm{ggT}(a, b) \mid \underbrace{(ax + by)}_{=c}$. $\square$

Folgerung: Ist $\mathrm{ggT}(a, b)$ kein Teiler von c, so hat $ax + by = c$ keine ganzzahlige Lösung.

Arbeitsblatt 1.2: Diophantische Gleichungen und ggT (Besprechung durch Schüler:in mit Presenter)

2. Der euklidische Algorithmus

Teilen mit Rest:

$13 : 4 = 3 \text{ R } 1$ bedeutet: $13 = 3 \cdot 4 + 1$

$223 : 25 = 8 \text{ R } 23$ bedeutet: $223 = 8 \cdot 25 + 23$

Satz (Teilen mit Rest): Seien $a, b \in \mathbb{N}_+$. Dann gibt es eindeutig bestimmte Zahlen $k, r \in \mathbb{N} = \{0, 1, \ldots\}$, so dass gilt:

$$a = kb + r \quad \text{und} \quad 0 \leq r \leq b - 1.$$

Anmerkung: Ohne die Bedingung $0 \leq r \leq b - 1$ sind k, r nicht eindeutig, z.B.

$$23 = 4 \cdot 5 + 3 \quad \text{und} \quad 23 = 3 \cdot 5 + 8.$$

Arbeitsblatt 1.3: Teilen mit Rest (Besprechung an Tafel durch Zuruf)

Euklidischer Algorithmus: Gesucht $\mathrm{ggT}(468, 60)$.

Teilen mit Rest:

$$\begin{aligned} 468 &= 7 \cdot 60 + 48 \\ 60 &= 1 \cdot 48 + 12 \\ 48 &= 4 \cdot 12 \end{aligned} \quad \Rightarrow \quad \mathrm{ggT}(468, 60) = 12$$

Stimmt das immer?

Satz: Sei $a = k \cdot b + r$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Beweis: 1) $\mathrm{ggT}(b, r)$ teilt b und r.

$\overset{\text{früherer Satz}}{\Rightarrow}$ $\mathrm{ggT}(b, r)$ teilt $a = k \cdot b + 1 \cdot r$

$\Rightarrow$ $\mathrm{ggT}(b, r)$ teilt a und b

$\Rightarrow$ $\mathrm{ggT}(b, r) \leq \mathrm{ggT}(a, b)$.

2) Löse die Gleichung nach r auf: $r = a - k \cdot b$.

Wie vorher folgt: $\mathrm{ggT}(a, b)$ teilt b und r

$\Rightarrow$ $\mathrm{ggT}(a, b) \leq \mathrm{ggT}(b, r)$.

1) und 2) $\Rightarrow$ $\mathrm{ggT}(b, r) = \mathrm{ggT}(a, b)$. $\square$

Euklidischer Algorithmus für $\mathrm{ggT}(98, 126)$:

$$\begin{array}{rcl} \overbrace{126}^{a} &=& 1 \cdot \overbrace{98}^{b} + \overbrace{28}^{r} \\ 98 &=& 3 \cdot 28 + 14 \\ 28 &=& 2 \cdot 14 \end{array} \quad \overset{\text{Satz}}{\Rightarrow} \quad \begin{array}{rcl} \mathrm{ggT}(\overbrace{126}^{a}, \overbrace{98}^{b}) &=& \mathrm{ggT}(\overbrace{98}^{b}, \overbrace{28}^{r}) \\ \mathrm{ggT}(98, 28) &=& \mathrm{ggT}(28, 14) \\ \mathrm{ggT}(28, 14) &=& 14 \\ \hline \mathrm{ggT}(126, 98) &=& 14 \end{array}$$

Arbeitsblatt 1.4: Euklidischer Algorithmus (Besprechung durch Schüler:in mit Presenter)

11.3 Arbeitsblätter

Siehe folgende Seiten

Diophantische Gleichungen

Aufgabe 1

Versuche, jeweils ganzzahlige Lösungen $(x \mid y)$ der angegebenen Gleichung zu finden.
Falls du vermutest, dass es keine Lösung gibt, begründe deine Vermutung.

a) $x + 3y = 10$:

b) $3x + 7y = 1$:

c) $18x + 12y = 3$:

Zusatzaufgaben:

d) $5x + 5y = 1$:

e) $5x + 15y = 50$:

f) $18x + 12y = 66$:

Diophantische Gleichungen und ggT

Aufgabe 2

Gegeben sind diophantische Gleichungen der Form $ax + by = c$. Bestimme jeweils die Menge der gemeinsamen Teiler von a und b, den $\mathrm{ggT}(a, b)$ und untersuche, ob $\mathrm{ggT}(a, b)$ Teiler von c ist. Falls es Lösungen gibt, vereinfache die Gleichung, indem Du beide Seiten durch die selbe geeignet gewählte Zahl teilst und rate eine Lösung $(x \mid y)$.

a) $18x + 12y = 24$:

Menge der gemeinsamen Teiler von 18 und 12: $\{\quad\}$,

$\mathrm{ggT}(12, 18) =$.

Die Gleichung ist

- ☐ nicht lösbar, denn
- ☐ lösbar, denn ich habe eine Lösung gefunden:
  - Vereinfachte Gleichung:
  - Eine Lösung: $(x \mid y) =$ $(\quad \mid \quad)$

.

b) $45x + 30y = 5$:

Menge der gemeinsamen Teiler von 45 und 30: $\{\quad\}$,

$\mathrm{ggT}(45, 30) =$.

Die Gleichung ist

- ☐ nicht lösbar, denn
- ☐ lösbar, denn ich habe eine Lösung gefunden:
  - Vereinfachte Gleichung:
  - Eine Lösung: $(x \mid y) =$ $(\quad \mid \quad)$.

Zusatzaufgabe 1

Gegeben ist die diophantische Gleichung $300x + 468y = 108$. Fülle die Kästchen aus.

Menge der gemeinsamen Teiler von 300 und 468: $\{\quad\}$,

$\mathrm{ggT}(300, 486) =$.

Die Gleichung ist

- ☐ nicht lösbar, denn
- ☐ lösbar, denn ich habe eine Lösung gefunden:
  - Vereinfachte Gleichung:
  - Eine Lösung: $(x \mid y) =$ $(\quad \mid \quad)$

Teilen mit Rest

Aufgabe 3

Teile jeweils a durch b mit Rest und schreibe die Lösung als Gleichung $a = k \cdot b + r$ auf.

a) $a = 143,\ b = 12$:

b) $a = 14130,\ b = 58$:

Zusatzaufgaben:

c) $a = 1\,111\,111,\ b = 2\,222$:

d) $a = 123\,321,\ b = 2\,010$:

Hinweis: Teil a) geht im Kopf, aber für die anderen Aufgabenteile ist ein Taschrechner hilfreich.

Euklidischer Algorithmus

Aufgabe 4

Berechne mit dem Euklidischen Algorithmus:

a) $\mathrm{ggT}(150, 54)$,

b) $\mathrm{ggT}(300, 468)$,

c) $\mathrm{ggT}(2717, 2431)$,

d) $\mathrm{ggT}(4263, 4641)$.

Zusatzaufgabe 2

Bestimme jeweils für die gegebene Gleichung $ax + y = c$ den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$. Vereinfache dann die gegebene Gleichung und suche möglichst viele verschiedene ganzzahlige Lösungen $(x \mid y)$. Kannst du ein Bildungsgesetz erkennen? Kannst Du eine Formel angeben, die alle Lösungen beschreibt?

a) $42x + 126y = 84$,

b) $81x + 54y = 27$.

Schriftliche Aufgaben

Name:

Aufgabe 5

Wahr oder falsch? Kreuze an!

	wahr	falsch
Der größte gemeinsame Teiler zweier Zahlen kann 1 sein.		
Der größte gemeinsame Teiler zweier Zahlen kann 0 sein.		
Der größte gemeinsame Teiler zweier Zahlen kann negativ sein.		
Der größte gemeinsame Teiler zweier Zahlen a, b kann mit b übereinstimmen.		
Der größte gemeinsame Teiler zweier Zahlen a, b ist immer kleiner als a.		
Die Gleichung $4x + 6y = 1$ hat mindestens eine Lösung $(x \mid y)$ mit rationalen Zahlen x, y.		
Die Gleichung $4x + 6y = 1$ hat mindestens eine Lösung $(x \mid y)$ mit ganzen Zahlen x, y.		
Die Gleichung $2x + 7y = 1$ hat mindestens eine Lösung $(x \mid y)$ mit ganzen Zahlen x, y.		
Seien x, y, a, b ganze Zahlen, a, b nicht beide 0. Dann gilt: $\mathrm{ggT}(a, b) \mid (ax+by)$.		

Aufgabe 6

Gegeben ist die Gleichung $4x + 5y = 1$. Gib drei verschiedene Lösungen $(x \mid y)$ mit ganzen Zahlen x, y an.

Lösungen: $(x \mid y) = \boxed{\left(\quad \middle| \quad\right)}$, $\boxed{\left(\quad \middle| \quad\right)}$, $\boxed{\left(\quad \middle| \quad\right)}$.

Weiter auf Seite 2

Aufgabe 7

Berechne den größten gemeinsamen Teiler der Zahlen 276 und 114 mit Hilfe des euklidischen Algorithmus.

Euklidischer Algorithmus:

$\Rightarrow\ \mathrm{ggT}(276, 114) =$

Aufgabe 8

Gegeben ist die diophantische Gleichung

$$63x + 147y \ = \ 105. \qquad (*)$$

a) Bestimme den größten gemeinsamen Teiler von 63 und 147.

$\mathrm{ggT}(63, 147) =$

b) Dividiere die Gleichung $(*)$ auf beiden Seiten durch $\mathrm{ggT}(63, 147)$ und gibt die Gleichung an, die dadurch entsteht. Sie besitzt die selben Lösungen wie $(*)$.

Neue Gleichung: $(**)$

c) Errate zwei verschiedene Lösungen $(x \mid y)$ von $(**)$, wobei x, y ganze Zahlen sind.

Lösungen: $(x \mid y) = \left(\ \middle|\ \right)$, $\left(\ \middle|\ \right)$.

d) **Zusatzaufgabe:** Gib alle Lösungen $(x \mid y)$ mit ganzen Zahlen x, y von $(**)$ an.

Alle Lösungen: $(x \mid y) =$

12 Ausarbeitung Unterrichtsstunde 2: Diophantische Gleichungen

12.1 Stundenverlauf

Zeit	Unterrichtsschritte bzw. Unterrichtsarrangement	Sozialform L-S-Tätigkeit Methode	Was ich brauche
17:00	Begrüßung und Wiederholung	Tafelvortrag	
17:03	Problemstellung, Existenzsatz und erweiterter euklidischer Algorithmus	Tafelvortrag, fragend-entwickelnd	
17:18	Übungs- und Entdeckungsphase, Ergebnisse an Tafel	Einzel-/ Partnerarbeit	Arbeitsblatt 2.1
17:28	Existenz einer Lösung: Satz, Beweis und Anwendung auf Problemstellung	Tafelvortrag, Beweis fragend entwickelnd	
17:38	Entdeckungsphase	Einzel-/ Partnerarbeit	Arbeitsblatt 2.2
17:48	Lösungsbesprechung mit Tabelle	Fragend-entwickelnd	
17:51	Alle Lösungen: Satz, Beweis Anwendung auf Problemstellung	Tafelvortrag Fragend-entwickelnd	
18:15	Übungsphase, Schüler:innen präsentieren Ergebnisse, Lösungen für Zusatzaufgabe auslegen	Einzel-/ Partnerarbeit	Arbeitsblatt 2.3 Visualizer Lösungsblatt
18.30	Verabschiedung		

Kommentar: Auch diese Stunde ist sehr voll.

12.2 Tafelanschriebe

Wiederholung:

Diophantische Gleichung: $ax + by = c$
$a, b, c \in \mathbb{N}$ gegeben, ganzzahlige Lösung $(x \mid y)$ gesucht.

Satz: Ist $\mathrm{ggT}(a, b)$ kein Teiler von c, dann gibt es keine Lösung der Gleichung.

3. Eine Lösung berechnen

Gesucht: Alle ganzzahligen Lösungen von $110x + 32y = 8$.

Satz: Zu beliebig gewählten natürlichen Zahlen a, b gibt es ganze Zahlen x, y, so dass

$$ax + by \;=\; \mathrm{ggT}(a, b).$$

Beispiel: Erweiterter Euklidischer Algorithmus für $110x + 32y \;=\; \mathrm{ggT}(110, 32)$.

Schritt 1:

$$\begin{aligned} 110 &= 3 \cdot 32 + 14 \\ 32 &= 2 \cdot 14 + 4 \\ 14 &= 3 \cdot 4 \;\; + 2 \\ 4 &= 2 \cdot 2 \end{aligned}$$

Schritt 2:

$$\begin{aligned} 14 &= 110 - 3 \cdot 32 \\ 4 &= 32 - 2 \cdot 14 \\ 2 &= 14 - 3 \cdot 4 \end{aligned}$$

$$\begin{aligned} \Rightarrow \;\; \mathrm{ggT}(110, 32) \;=\; 2 &= 14 - 3(\overbrace{32 - 2 \cdot 14}^{4=}) \\ &= 14 - 3 \cdot 32 + 6 \cdot 14 \;=\; 7 \cdot 14 - 3 \cdot 32 \\ &= 7(\overbrace{110 - 3 \cdot 32}^{14=}) - 3 \cdot 32 \;=\; 7 \cdot 110 - 21 \cdot 32 - 3 \cdot 32 \\ &= 7 \cdot 110 - 24 \cdot 32 \end{aligned}$$

$\Rightarrow$ $(x \mid y) = (7 \mid -24)$ ist eine Lösung.

Arbeitsblatt 2.1: Eine Lösung berechnen (Besprechung an Tafel)

Satz: Seien $a, b, c \in \mathbb{N}$ gegeben, so dass $\mathrm{ggT}(a, b) \mid c$. Dann hat

$$ax + by \;=\; c \;=\; n \cdot \mathrm{ggT}(a, b)$$

mindestens eine ganzzahlige Lösung $(x \mid y)$.

Beweis: Es gibt ein $n \in \mathbb{N}$, so dass $c = n \cdot \mathrm{ggT}(a, b)$.

Letzter Satz $\Rightarrow$ es gibt ganzzahlige x, y mit

$$\begin{aligned} & ax + by \;=\; \mathrm{ggT}(a, b) && \mid \cdot n \\ \Leftrightarrow \;\; & n(ax + by) \;=\; n \cdot \mathrm{ggT}(a, b) \\ \Leftrightarrow \;\; & a(nx) + b(ny) \;=\; c \\ \Rightarrow \;\; & (nx \mid ny) \text{ ist ganzzahlige Lösung.} \end{aligned}$$

□

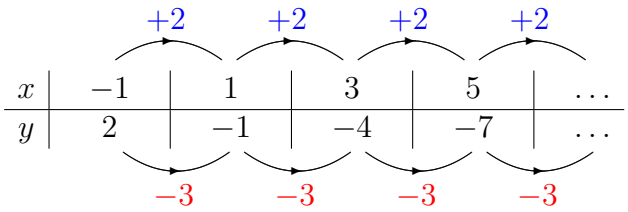
Beispiel: $110x + 32y = \mathrm{ggT}(110, 32) = 2$ hat die Lösung $(7 \mid -24)$.

$\Rightarrow$ $110x + 32y = 8 = 4 \cdot 2$ hat die Lösung $(4 \cdot 7 \mid 4 \cdot (-24)) = (28 \mid -96)$.

Arbeitsblatt 2.2: Mehrere Lösungen finden (Besprechung an Tafel)

4. Alle Lösungen berechnen

Beobachtung: Die Gleichung $3x + 2y = 1$ hat die Lösungen



D.h. x wird in 2er Schritten erhöht und y in 3er Schritten erniedrigt.

Satz: 1) Ist $(x_0 \mid y_0)$ eine Lösung von $ax + by = c$, dann sind alle Zahlenpaare

$$(x \mid y) \;=\; (x_0 + k \cdot b \mid y_0 - k \cdot a) \text{ mit } k \in \mathbb{Z} \qquad (*)$$

ebenfalls Lösungen.

2) Gilt $\mathrm{ggT}(a, b) = 1$, dann sind durch $(*)$ alle Lösungen gegeben.

Beweis: 1) Durch $(*)$ sind Lösungen gegeben, denn

$ax + by \;=\; a(x_0 + kb) + b(y_0 - ka) \;=\; ax_0 + \cancel{akb} + by_0 - \cancel{bka} \;=\; c.$

2) Sei $(x \mid y)$ irgendeine Lösung von $ax + by = c$.

Es gilt $a(x - x_0) + b(y - y_0) \;=\; ax + by - (ax_0 + by_0) \;=\; c - c \;=\; 0$

$\Rightarrow\; b(y - y_0) \;=\; -a(x - x_0).$

$\mathrm{ggT}(a, b) = 1 \;\Rightarrow\; b \mid (x - x_0) \;\Rightarrow\; x - x_0 = k \cdot b$ mit geeignetem $k \in \mathbb{Z}$.

$\Rightarrow\; y - y_0 \;=\; -\frac{a}{b}(x - x_0) \;=\; -\frac{a}{b} \cdot k \cdot b \;=\; -k \cdot a.$

$\Rightarrow\; y \;=\; y_0 - k \cdot a, \quad x \;=\; x_0 + k \cdot b$

$\Rightarrow\; (x \mid y)$ wird durch die Formel $(*)$ beschrieben. □

Beispiel: $110\,x + 32\,y = 8$ (1)

hat die Lösung $(x_0 \mid y_0) = (28 \mid -96)$.

1) des Satzes: $(x \mid y) = (28 - k \cdot 32 \mid -96 + k \cdot 110)$ mit $k \in \mathbb{Z}$ sind Lösungen.

Teile die Gleichung (1) auf beiden Seiten durch $2 = \mathrm{ggT}(110, 32)$:

$$55\,x + 16\,y \;=\; 4 \qquad (2)$$

hat die selben Lösungen wie (1), und $\mathrm{ggT}(55, 16) = 1$.

2) des Satzes: Alle Lösungen von (2) sind

$$(x \mid y) = (28 + k \cdot 16 \mid -96 - k \cdot 55) \text{ mit } k \in \mathbb{Z}.$$

Dies sind auch alle Lösungen von (1).

Arbeitsblatt 2.3: Alle Lösungen bestimmen (Besprechung an Tafel)

12.3 Arbeitsblätter

Siehe folgende Seiten

Eine Lösung berechnen

Aufgabe 1

Bestimme jeweils eine ganzzahlige Lösung $(x \mid y)$ der angegebenen Gleichung. Berechne dazu in den Aufgabenteilen a) und d) zunächst den ggT der Koeffizienten mit Hilfe des euklidischen Algorithmus. Erweitere dann den Algorithmus, um eine Lösung zu finden.

a) $96x + 66y = 6$,

b) $96x + 66y = 18$ (verwende hierzu die Lösung aus Teil a)),

c) Für beliebiges fest vorgegebenes $n \in \mathbb{N}$: $96x + 66y = n \cdot 6$ (auch hier erweist sich die Lösung aus Teil a) als nützlich),

d) **Zusatzaufgabe:** $119x + 143y = 1$,

e) **Zusatzaufgabe:** $119x + 143y = 4$.

Mehrere Lösungen finden

Aufgabe 2

Bestimme durch Probieren mehrere ganzzahlige Lösungen $(x \mid y)$, möglichst alle.

a) $3x + 2y = 1$:

Zusatzaufgabe:

b) $3x + 9y = 3$:

Alle Lösungen bestimmen

Aufgabe 3

Gegeben ist die Gleichung

$$144x + 52y \;=\; 8. \qquad (*)$$

a) Bestimme $\mathrm{ggT}(144, 52)$ mit Hilfe des euklidischen Algorithmus.

b) Erweitere den euklidischen Algorithmus und berechne eine ganzzahlige Lösung $(x \mid y)$ der Gleichung $144x + 52y = \mathrm{ggT}(144, 52)$.

c) Berechne eine Lösung von $(*)$.

d) Teile die Gleichung $(*)$ auf beiden Seiten durch $\mathrm{ggT}(144, 52)$ und gib die Gleichung an, die dadurch ensteht.

e) Gib alle ganzzahligen Lösungen von $(*)$ an.

Zusatzaufgabe 1

Bestimme alle Lösungen für die Gleichungen aus Aufgabe 1 dieser Einheit (siehe Arbeitsblatt 1).

Alle Lösungen bestimmen (mit Lösungen)

Zusatzaufgabe 1

Bestimme alle Lösungen für die Gleichungen aus Aufgabe 1 dieser Einheit (siehe Arbeitsblatt 1).

a) $96x + 66y = 6$,

b) $96x + 66y = 18$,

c) Für beliebiges fest vorgegebenes $n \in \mathbb{N}$: $96x + 66y = n \cdot 6$,

d) **Zusatzaufgabe:** $119x + 143y = 1$,

e) **Zusatzaufgabe:** $119x + 143y = 4$.

Lösung:

a) Aus der Aufgabe 1a ist bekannt: Eine Lösung ist $(x \mid y) = (-2 \mid 3)$. Teile die Gleichung durch $\mathrm{ggT}(96, 66) = 6$:

$$96x + 66y = 6 \;\Leftrightarrow\; 16x + 11y = 1.$$

Wegen $\mathrm{ggT}(16, 11) = 1$ sind nach dem letzten Satz alle Lösungen gegeben durch

$$(x \mid y) \;=\; (-2 + 11k \mid 3 - 16k), \quad (k \in \mathbb{Z}).$$

b) Genauso: Eine Lösung ist $(x \mid y) = (-6 \mid 9)$. Teile die Gleichung durch 6: $16x + 11y = 3$. Alle Lösungen:

$$(x \mid y) \;=\; (-6 + 11k \mid 9 - 16k), \quad (k \in \mathbb{Z}).$$

Beachte, dass nur der Teil der Lösung aus Teil a), der nicht den Faktor k enthält, mit 3 multipliziert wird!

c) Genauso: Alle Lösungen $(x \mid y) = (-2n + 11k \mid 3n - 16k)$, $(k \in \mathbb{Z})$.

d) Wegen $\mathrm{ggT}(143, 119) = 1$ sind bereits die Voraussetzungen des letzten Satzes erfüllt. Eine Lösung ist $(x \mid y) = (-6 \mid 5)$.

$\Rightarrow\; (x \mid y) = (-6 + 143k \mid 5 - 119k)$ mit $k \in \mathbb{Z}$ sind alle Lösungen.

e) Alle Lösungen sind $(x \mid y) = (-24 + 143k \mid 20 - 119k)$ mit $k \in \mathbb{Z}$.

Schriftliche Aufgaben

Name:

Aufgabe 3

Wahr oder falsch? Kreuze an!

	wahr	falsch
Die diophantische Gleichung $ax+by=c$ besitzt entweder keine oder unendlich viele ganzzahlige Lösungen $(x \mid y)$.		
Gilt $\mathrm{ggT}(a,b) \mid c$, dann hat die Gleichung $ax+by=c$ genau eine ganzzahlige Lösung $(x \mid y)$.		
Gilt $\mathrm{ggT}(a,b) \mid c$, dann hat die Gleichung $ax+by=c$ unendlich viele ganzzahlige Lösungen $(x \mid y)$.		
Hat die diophantische Gleichung $ax+by=c$ mindestens eine ganzzahlige Lösung $(x \mid y)$, so folgt $\mathrm{ggT}(a,b) \mid c$.		
Mit dem erweiterten euklidischen Algorithmus berechnet man eine ganzzahlige Lösung $(x \mid y)$ von $ax+by=\mathrm{ggT}(a,b)$.		
Mit dem erweiterten euklidischen Algorithmus berechnet man alle ganzzahligen Lösungen $(x \mid y)$ von $ax+by=\mathrm{ggT}(a,b)$.		
Ist $(x_0 \mid y_0)$ eine ganzzahlige Lösung von $ax+by=c$, so sind alle Lösungen durch $(x_0+kb \mid y_0-ka)$ mit $k \in \mathbb{Z}$ gegeben.		
Ist $(x_0 \mid y_0)$ eine ganzzahlige Lösung von $ax+by=\mathrm{ggT}(a,b)$, so ist $(x \mid y)=(5x_0 \mid 5y_0)$ eine Lösung von $ax+by=5\mathrm{ggT}(a,b)$.		

Aufgabe 4

Gegeben ist die diophantische Gleichung

$$71x+43y \;=\; 2. \qquad (*)$$

a) Die Zahlen $a=71$ und $b=43$ sind Primzahlen. Gib den größten gemeinsamen Teiler an.

$\mathrm{ggT}(71,43) =$ ☐.

b) Warum ist $(x \mid y)=(-3 \mid 5)$ eine Lösung von $(*)$?

☐

c) Gib alle Lösungen der Gleichung $(*)$ an.

Alle Lösungen $(x \mid y) =$ ☐.

d) Gib alle Lösungen der Gleichung $71x+43y=8$ an.

Alle Lösungen $(x \mid y) =$ ☐.

Weiter auf Seite 2

Aufgabe 5

Gegeben ist die diophantische Gleichung

$$108x + 300y \;=\; 60. \qquad (*)$$

a) Führe den erweiterten euklidischen Algorithmus durch, um $\mathrm{ggT}(108, 300)$ und eine ganzzahlige Lösung $(x \mid y)$ der Gleichung $108x + 300y = \mathrm{ggT}(108, 300)$ zu erhalten.

Schritt 1:

Schritt 2:

$\mathrm{ggT}(108, 300) =$

Eine Lösung der Gleichung $108x + 300y = \mathrm{ggT}(108, 300)$: $(x \mid y) =$.

b) Gib eine Lösung von $(*)$ an. Lösung: $(x \mid y) =$.

c) Vereinfache die Gleichung $(*)$, indem Du sie durch eine möglichst große Zahl teilst.

Vereinfachte Gleichung: .

Für die Lösungen von $(*)$ und die Lösungen der vereinfachten Gleichung gilt:

.

d) Gib alle Lösungen von $(*)$ an.

Alle Lösungen von $(*)$: $(x \mid y) =$.

Zusatzmaterial

Zusatzaufgabe 2

Bestimme alle Lösungen der Gleichung $144x + 400y = 48$.

Zusatzaufgabe 3

Ein zerstreuter Bankkassierer verwechselte 1-Euromünzen und 1-Centmünzen, als er den Scheck von Herrn Krause auszahlte, indem er ihm 1-Euromünzen anstelle von 1-Centmünzen und 1-Centmünzen anstelle von 1-Euromünzen gab. Nachdem Herr Krause zuhause großzügig 5 Cent in die Spardose seines Sohnes getan hatte, entdeckte er, dass er jetzt noch genau doppelt so viel Geld hatte, wie auf dem Scheck stand. Auf welche Summe war der Scheck ausgestellt?

Zusatzaufgabe 4

Gib alle natürlichen Zahlen an, die bei Division durch 19 den Rest 3 und gleichzeitig bei Division durch 29 den Rest 18 lassen.

Hinweis: Die erste Bedingung lässt sich als Gleichung $x = k \cdot 19 + 3$ formulieren, entsprechend die zweite Bedingung als $x = -l \cdot 29 + 18$ (mit negativem l). Eliminiere zunächst x und löse die entstehende diophantische Gleichung. Beachte, dass nur natürliche Zahlen gesucht sind.

Zusatzaufgabe 5

Gegeben sind zwei natürliche Zahlen a, b mit den Darstellungen

$$a \;=\; p_1^3 \cdot p_2 \cdot p_3^4, \quad b \;=\; p_1^2 \cdot p_3 \cdot p_4^2,$$

wobei $p_1, \ldots, p_4$ paarweise verschiedene Primzahlen sind. Man nennt diese Darstellung **Primfaktorzerlegung**.

a) Wie kann man aus dieser Darstellung $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ ausrechnen?

b) Wie hängen $a \cdot b$, $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ zusammen?

13 Ausarbeitung Unterrichtsstunde 3: Kongruenzen

13.1 Stundenverlauf

Zeit	Unterrichtsschritte bzw. Unterrichtsarrangement	Sozialform L-S-Tätigkeit Methode	Was ich brauche
17:00	Begrüßung		
17:01	Teilbarkeit durch 9	Einzel-/ Partnerarbeit	Arbeitsblatt 3.1
17:06	Kongruenz: Definition und äquivalente Aussagen	Tafelvortrag	
17:30	Übung: Kongruenzen	Einzel-/ Partnerarbeit	Arbeitsblatt 3.2
17:43	Rechenregeln für Kongruenzen	Tafelvortrag	
17:56	Übung Besprechung durch Schüler:in am Visualizer	Einzel-/ Partnerarbeit	Arbeitsblatt 3.3
18:15	Quersummenregel	Tafelvortrag	
18:25	Umkehraufgabe zur Quersummenregel	Einzel-/ Partnerarbeit	Arbeitsblatt 3.4
18.30	Verabschiedung		

Kommentar: Viel Text, wenig Aufgaben, viele Beweise.

13.2 Tafelanschriebe

Arbeitsblatt 3.1: Teilen durch 9 (Besprechung an Tafel)

$34:$ Quersumme $= 7$, $34 : 9 = 3\text{R}7$

$349:$ QS $= 16$, $349 : 9 = 38\text{R}7$

$$\begin{array}{r} -\,27 \\ \hline 79 \\ -72 \\ \hline 7 \end{array}$$

5. Kongruenzen

Definition: Seien a, b ganze Zahlen, $m \in \mathbb{N}_+ = \{1, 2, \ldots\}$. Schreibe

$$a \equiv b \mod m \qquad (a \text{ ist kongruent zu } b \text{ modulo } m),$$

falls $a - b$ durch m teilbar ist.

Beispiel: $15 \equiv 3 \mod 6$, denn $15 - 3 = 12$ ist durch 6 teilbar.

Satz (Kongruenzkriterien): Folgende Aussagen sind äquivalent:

(1) $a \equiv b \mod m$
(2) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$
(3) a und b lassen beim Teilen durch m den selben Rest.

Beweisprinzip Ringschluss:

$$\begin{array}{ccc} & (1) & \\ \nearrow & & \searrow \\ (3) & \Longleftarrow & (2) \end{array}$$

Beweis: (1) $\Rightarrow$ (2):

$$\begin{aligned} a \equiv b \mod m &\Leftrightarrow m \mid (a-b) \\ &\Rightarrow \text{Es gibt ein } k \in \mathbb{Z}, \text{ so dass } a - b = k \cdot m \quad \big| + b \\ &\Rightarrow a = km + b = b + km \end{aligned}$$

(2) $\Rightarrow$ (3): Sei r der Rest beim Teilen von b durch m,
d.h. $b = lm + r$ mit einem $l \in \mathbb{Z}$.

$$\begin{aligned} (2) \Rightarrow a &= b + km \\ &= lm + r + km \\ &= \underbrace{(l+k)}_{\in \mathbb{Z}} m + r \end{aligned}$$

$\Rightarrow$ a lässt beim Teilen durch m den selben Rest r wie b.

(3) $\Rightarrow$ (1): $a = km + r,\ b = lm + r$ mit $k, l \in \mathbb{Z}$

$$\begin{aligned} \Rightarrow\ a - b &= km + r - (lm + r) \\ &= km + \cancel{r} - kl - \cancel{r} \\ &= (k - l)m \\ \Rightarrow\ m &\mid (a - b) \\ \Leftrightarrow\ a &\equiv b \mod m \end{aligned}$$ □

Aus Aufgabe 1: b) $2005 : 9 = 222$ R 7
$\Leftrightarrow 2005 = 9 \cdot 222 + 7$
$\Rightarrow 2005 \equiv 7 \mod 9$

c) $2050 \equiv 7 \mod 9$
$\Rightarrow\ 2050 \equiv 2005 \mod 9$

Arbeitsblatt 3.2: Kongruenzgleichungen (Besprechung an Tafel durch Zuruf)

Satz (Rechenregeln für Kongruenzen):

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann:

$$\begin{aligned} &\text{a}_1) && -a \equiv -b && \mod m \\ &\text{a}_2) && a + c \equiv b + d && \mod m \\ &\text{a}_3) && ac \equiv bd && \mod m \\ &\text{a}_4) && a^2 \equiv b^2 && \mod m,\ a^3 \equiv b^3 \mod m,\ \ldots \end{aligned}$$

b) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann

$$\begin{aligned} &\text{b}_1) && a \equiv a && \mod m \\ &\text{b}_2) && b \equiv a && \mod m \\ &\text{b}_3) && a \equiv c && \mod m \end{aligned}$$

Beweis von a_3): Wir wissen $a = b + km,\ c = d + lm$ mit $k, l \in \mathbb{Z}$.
Wir suchen ein $j \in \mathbb{Z}$, so dass $ac = bd + jm$.

$$\begin{aligned} ac &= (b + km)(d + lm) \\ &= bd + blm + kmd + kmlm \\ &= bd + \underbrace{(bl + kd + klm)}_{\in\mathbb{Z}} m \\ \Rightarrow\ ac &= bd + jm \\ \Rightarrow\ ac &\equiv bd \mod m \end{aligned}$$ □

Arbeitsblatt 3.3: Rechenregeln für Kongruenzen (Schüler:innenlösungen am Visualizer)

Satz (Quersummenregel): Wir schreiben $Q(a)$ für die Quersumme einer natürlichen Zahl a. Wir bilden so lange die Quersummen $Q(a),\ Q(Q(a)), \ldots$, bis sich eine Zahl b zwischen 1 und 9 ergibt. Dann gilt $a \equiv b \mod 9$.
Wenn $b = 9$, dann ist a durch 9 teilbar.

Beispiel: $a = 123456$: $Q(a) = 21,\ Q(Q(a)) = 3\ \Rightarrow\ 123456 \equiv 3 \mod 9$

Beweis 1) $a \equiv Q(a) \mod 9$:

Eine natürliche Zahl a mit $n+1$ Stellen können wir darstellen als

$$a = \begin{array}{|c|c|}\hline a_n & a_{n-1} \\ \hline \end{array} \ldots \begin{array}{|c|c|c|}\hline a_2 & a_1 & a_0 \\ \hline \mathsf{H} & \mathsf{Z} & \mathsf{E} \\ \hline \end{array} \Rightarrow a = \underbrace{a_0 \cdot 1}_{\equiv a_0} + \underbrace{a_1 \cdot 10}_{\equiv a_1} + \underbrace{a_2 \cdot 100}_{\equiv a_2} + \ldots + \underbrace{a_n \cdot 10^n}_{\equiv a_n \bmod 9}.$$

$$\begin{array}{rcl} 10 & \equiv & 1 \bmod 9 \\ 10^2 & \equiv & 1^2 \bmod 9 \\ \vdots & & \\ 10^n & \equiv & 1 \bmod 9 \end{array} \quad \overset{\text{Satz a}_3)}{\Rightarrow} \quad \begin{array}{rcl} a_1 \cdot 10 & \equiv & a_1 \cdot 1 \bmod 9 \\ a_2 \cdot 10^2 & \equiv & a_2 \cdot 1 \bmod 9 \\ & \vdots & \\ a_n \cdot 10^n & \equiv & a_n \cdot 1 \bmod 9 \end{array}$$

$$\overset{\text{Satz a}_2)}{\Rightarrow} \quad a \equiv \underbrace{a_0 + a_1 + a_2 + \ldots + a_n}_{=Q(a)} \mod 9.$$

2) $a \equiv Q(a), Q(a) \equiv Q(Q(a)) \overset{\text{Satz b}_3)}{\Rightarrow} a \equiv Q(Q(a)) \Rightarrow a \equiv Q(Q(Q(a))) \ldots$ □

Arbeitsblatt 3.4: Die Quersummenregel (Besprechung an Tafel durch Zuruf)

13.3 Arbeitsblätter

Siehe folgende Seiten

Teilen durch 9

Aufgabe 1

Bestimme den Rest beim Teilen durch 9.

a) 1000: **b)** 2005: **c)** 2050:

d) 1035: **e)** 5103:

Zusatzaufgabe 1

Bestimme eine vierstellige, eine fünfstellige und eine sechsstellige Zahl, die beim Teilen durch 9 den Rest 3 lassen.

Kongruenzgleichungen

Aufgabe 2

Bestimme jeweils das Ergebnis beim Teilen mit Rest. Trage Deine Lösungen in die Kästchen ein.

a) $33 = \square \cdot 6 + \square$

$\Rightarrow 33 \equiv \square \mod 6$

b) $-101 = \square \cdot 4 + \square$

$\Rightarrow -101 \equiv \square \mod 4$

Aufgabe 3

Bestimme möglichst alle ganzzahligen Lösungen x der folgenden Gleichungen.

a) $5 + x \equiv 2 \mod 7$: $L =$

b) $5 \cdot x \equiv 2 \mod 7$: $L =$

Zusatzaufgabe 2

Bestimme möglichst alle ganzzahligen Lösungen x der folgenden Gleichungen.

a) $5 \cdot x \equiv 2 \mod 10$:

b) $-34 \equiv x \mod 5$:

Rechenregeln für Kongruenzen

Aufgabe 4

Beweise die folgenden Aussagen:

a) Wenn $a \equiv b \mod m$ und $c \equiv d \mod m$, dann $a + c \equiv b + d \mod m$.

b) Wenn $a \equiv b \mod m$, dann $-a \equiv -b \mod m$.

c) Wenn $a \equiv b \mod m$ und $b \equiv c \mod m$, dann $a \equiv c \mod m$.

Hinweise: Zum Beweis von Teil a) kannst Du den Beweis von a_3), der an der Tafel steht, entsprechend anpassen.
Zum Beweis einer Kongruenz $a \equiv b \mod m$ genügt es, eine der folgenden drei äquivalenten Bedingungen nachzuweisen.

(1) $a - b$ ist durch m teilbar bzw. $a - b = km$ für ein $k \in \mathbb{Z}$
(2) Es gibt ein $k \in \mathbb{Z}$, so dass $a = b + km$
(3) a und b lassen beim Teilen durch m den selben Rest.

Die Quersummenregel

Aufgabe 5

Gib zwei verschiedene 10-stellige Zahlen an, deren Ziffern nur aus Achten und Nullen bestehen, und die beim Teilen durch 9 den Rest 3 ergeben.

Schriftliche Aufgaben

Name:

Aufgabe 6

Wahr oder falsch? Kreuze an!

	wahr	falsch
Die Gleichung $2x \equiv 10 \mod 3$ besitzt mindestens eine Lösung $x \in \mathbb{Z}$.		
Die Gleichung $2x \equiv 10 \mod 3$ besitzt unendlich viele Lösungen $x \in \mathbb{Z}$.		
Die Gleichung $2x \equiv 7 \mod 4$ besitzt mindestens eine Lösung $x \in \mathbb{Z}$.		
Die Gleichung $2x \equiv 7 \mod 4$ besitzt unendlich viele Lösungen $x \in \mathbb{Z}$.		
Aus $x \equiv 3 \mod 5$ und $y \equiv 6 \mod 5$ folgt $xy \equiv 30 \mod 5$.		
Aus $x \equiv 5 \mod 3$ folgt $2x \equiv 10 \mod 6$.		
Aus $x \equiv 5 \mod 3$ folgt $2x \equiv 5 \mod 6$.		
Aus $x \equiv 5 \mod 3$ folgt $2x \equiv 10 \mod 3$.		
Für jede natürliche Zahl x gilt $x \equiv 0 \mod x$.		
Für jede natürliche Zahl x gilt $2x \equiv -x \mod x$.		

Aufgabe 7

Gib die Menge L aller Lösungen der Kongruenzgleichung $3 \cdot x \equiv 1 \mod 11$ an.

$L =$ ☐.

Aufgabe 8

Mit $Q(x)$ wird die Quersumme der Zahl x bezeichnet. Gegeben ist die Zahl $a = 999\,888\,772$.

a) Berechne die angegebenen Quersummen.

$Q(a) =$ ☐, $Q(Q(a)) =$ ☐, $Q(Q(Q(a))) =$ ☐.

b) Gib jeweils eine möglichst kleine natürliche Zahl an, so dass die angegebene Kongruenz gilt.

$a \equiv$ ☐ $\mod 9$, $a \equiv$ ☐ $\mod 3$.

Weiter auf Seite 2

Aufgabe 9

In dieser Aufgabe kannst Du alle Lösungen der Kongruenzgleichung

$$37 \cdot x \equiv 1 \mod 7 \qquad (*)$$

systematisch bestimmen.

a) Zunächst sollst Du die Kongruenzgleichung umformen. Das Äquivalenzzeichen bedeutet hier, dass sich die Lösungsmenge nicht ändert. Fülle die Kästchen aus.

$37 \cdot x \equiv 1 \mod 7$

$\Leftrightarrow$ Es gibt ein $k \in \mathbb{Z}$, so dass $37 \cdot x = 1 + \square$

$\Leftrightarrow$ Es gibt ein $k \in \mathbb{Z}$, so dass $\square \cdot x - \square \cdot k = 1$

b) Bestimme mit dem erweiterten euklidischen Algorithmus eine Lösung der diophantischen Gleichung $37x + 7y = 1$.

Schritt 1:

Schritt 2:

$\mathrm{ggT}(37, 7) = \square$

Eine Lösung der Gleichung $37x + 7y = 1$: $(x \mid y) = \square$.

c) Gib alle Lösungen der diophantischen Gleichung $37x + 7y = 1$ an.

$(x \mid y) = \square$ mit $l \in \mathbb{Z}$.

d) Gib alle Lösungen der diophantischen Gleichung $37x - 7k = 1$ an.

$(x \mid y) = \square$ mit $l \in \mathbb{Z}$.

e) Gib die Lösungsmenge der Gleichung $(*)$ an.

$L = \square$.

Die Neunerprobe

Die Neunerprobe kann folgendermaßen zur Kontrolle von Rechenergebnissen benützt werden: Man benützt

$$\left.\begin{array}{rcl} a & \equiv & Q(a) \\ b & \equiv & Q(b) \end{array}\right\} \Rightarrow\ ab \equiv Q(ab) \text{ und } a+b \equiv Q(a+b)$$

Frage: $12345 \cdot 54321 \stackrel{?}{=} 671592745$
Neunerprobe: $12345 \equiv 6 \mod 9 \wedge 54321 \equiv 6 \mod 9 \Rightarrow 12345 \cdot 54321 \equiv 36 \equiv 9 \mod 9$
Aber $671592745 \equiv 46 \equiv 10 \equiv 1 \mod 9$

Also ist das Ergebnis falsch.

Zusatzaufgabe 3

Welche der folgenden Gleichungen sind garantiert falsch? (Ohne Taschenrechner!)

a) $12345 \cdot 54321 \stackrel{?}{=} 670592745$,

b) $6613598 \cdot 55500710 \stackrel{?}{=} 367359384654580$,

c) $6613598 \cdot 55500710 \stackrel{?}{=} 367059384654580$,

d) $6613598 \cdot 55500710 \cdot 432 \stackrel{?}{=} 158569654170778570$,

e) $123456709 + 6789402 + 878787487 + 1232123 \stackrel{?}{=} 1010365721$,

f) $123456709 + 6789402 + 878787487 + 1232123 \stackrel{?}{=} 1010265721$.

Zusatzmaterial

Zusatzaufgabe 4

Gegeben ist folgende Behauptung für $n \in \mathbb{Z}$:

$$\text{Entweder gilt } n^4 \equiv 1 \mod 5 \text{ oder } n^4 \equiv 0 \mod 5. \qquad (*)$$

a) Rechne nach, dass die Behauptung $(*)$ für $n = 1, 2, 3, 4, 5$ wahr ist.

b) Beweise mit den Rechenregeln für Kongruenzen: $a \equiv b \mod m \Rightarrow a^4 \equiv b^4 \mod m$.

c) Beweise, dass die Behauptung $(*)$ für alle $n \in \mathbb{Z}$ gilt.

Hinweis: Betrachte als erstes den Fall, dass $n = 5k + 1$ mit einem geeigneten $k \in \mathbb{Z}$ gilt. Welche Fälle müssen noch untersucht werden?

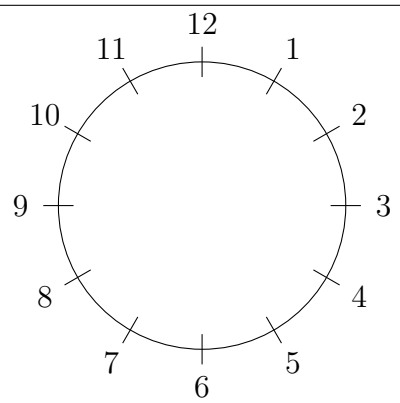
14 Ausarbeitung Unterrichtsstunde 4: Der Zahlenring

14.1 Stundenverlauf

Zeit	Unterrichtsschritte bzw. Unterrichtsarrangement	Sozialform L-S-Tätigkeit Methode	Was ich brauche
17:00	Die Uhr und die Fünfer-Uhr	Vortrag/ L-S-Gespräch	Tafel
17:05	Definition Restklasse, Restklassenring	Vortrag/ Beispiele L-S-Gespräch	Tafel
17:15	Kurze Übungsphase, Besprechung durch Zuruf	Einzel-/ Partnerarbeit	Arbeitsblatt 4.1
17:20	Addition und Multilplikation von Restklassen	Vortrag/ Beispiele L-S-Gespräch	Tafel
17:30	Übungsphase, Schüler:in präsentiert Lösung	Einzel-/ Partnerarbeit	Arbeitsblatt 4.2 Visualizer
17:40	Subtraktion und Division aus Verknüpfungstabellen	Vortrag/ L-S-Gespräch	Tafel
17:50	Übungsphase, Besprechung mit Visualizer	Einzel-/ Partnerarbeit	Arbeitsblatt 4.3 Visualizer
18:07	Existenz von Brüchen	Vortrag	Tafel
18:25	Übungsblatt austeilen		Arbeitsblatt 4.4
18.30	Verabschiedung		

Kommentar: Diese Einheit enthält viel Text zum Schreiben. Deshalb auf knappe Formulierungen achten. Ohne das vierte Arbeitsblatt sehr gut machbar. Das vierte Arbeitsblatt wurde im Online-Kurs verwendet, im Präsenz-Kurs nur am Schluss ausgeteilt.

14.2 Tafelanschriebe



Auf der Uhr: 4 Uhr + 5 Stunden = 9 Uhr
9 Uhr + 5 Stunden = 2 Uhr

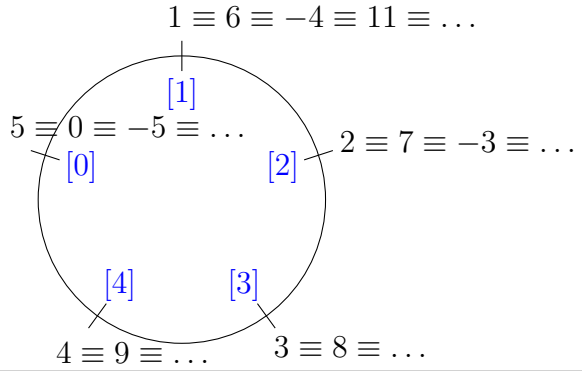
Auf der Uhr gilt 14 Uhr = 2 Uhr.

Mathematisch: $14 \equiv 2 \mod 12$, denn

14 und 2 lassen beim Teilen durch 12 den selben Rest
$12 \mid (14 - 2)$
$14 = 1 \cdot 12 + 2$

6. Rechnen mit Restklassen

Der Zahlenring modulo 5:



Betrachte alle Zahlen, die beim Teilen durch eine Zahl $m \in \mathbb{N}_+$ den selben Rest lassen. Diese Zahlen werden zu einer Menge zusammengefasst, der Restklasse.

Definition: Die Restklasse $[a]$ von a modulo m ist definiert durch

$$[a] := \{b \in \mathbb{Z} : b \equiv a \mod m\}.$$

a heißt Repräsentant der Restklasse $[a]$.

Beispiele modulo 5:

$$\begin{array}{lllllll} [0] & = & \{\ldots,-10,-5,0,5,10,\ldots\} & = & [5] & = & \ldots \\ [1] & = & \{\ldots,-9,-4,1,6,11,\ldots\} & = & [6] & = & [-4] \quad = \quad \ldots \\ [2] & = & \ldots & & & & \\ [3] & = & \ldots \quad = \quad [8] \quad = \quad \ldots & & & & \\ [4] & = & \ldots & & & & \end{array}$$

0 und 5 sind verschiedene Repräsentanten von $[0]$.

Definition: Die Menge aller Restklassen modulo m heißt Restklassenring modulo m, schreibe $\mathbb{Z}_m$.

Beispiel: $\mathbb{Z}_5 = \{[0],[1],[2],[3],[4]\}$.

Arbeitsblatt 4.1: Restklassen (Besprechung an Tafel)

Definition: Für $a, b \in \mathbb{Z}$ definiert man

$$\begin{array}{rcl} [a]+[b] & := & [a+b] \\ [a]\cdot[b] & := & [ab] \end{array}$$

Beispiele modulo 5:

$$\begin{array}{rcccl} [2]+[2] & = & [4] & & \\ [3]+[4] & = & [7] & = & [2] \\ [3]\cdot[4] & = & [12] & = & [2] \\ [-2]\cdot[-1] & = & [2] & & \\ [8]\cdot[9] & = & [72] & = & [2] \end{array}$$

Satz: Ist $[a]=[a']$ und $[b]=[b']$, so gilt $[a\cdot b]=[a'\cdot b']$ und $[a+b]=[a'+b']$.

Beweis: Ist $[a]=[a']$ und $[b]=[b']$, so folgt:

$$\begin{array}{rl} & a \equiv a' \mod m \quad \text{und} \quad b \equiv b' \mod m \\ \overset{\text{Rechenregeln für Kongruenzen}}{\Rightarrow} & ab \equiv a'b' \mod m \quad \text{und} \quad a+b \equiv a'+b' \mod m \\ \Rightarrow & [ab]=[a'b'] \quad \text{und} \quad [a+b]=[a'+b'] \end{array}$$ □

Arbeitsblatt 4.2: Rechnen mit Restklassen (Besprechung an Tafel)

In $\mathbb{Z}_5$: $[1]-[2] =$

$[1]-[4] =$

$\dfrac{[1]}{[2]} =$

$\dfrac{[2]}{[3]} =$

Aus der Additionstabelle für $\mathbb{Z}_5$: $[4]+[2]=[1]$

$$\Rightarrow \begin{cases} [1]-[2] = [4] = [-1] \\ [1]-[4] = [2] = [-3] \end{cases}$$

Satz: für $a, b \in \mathbb{Z}$ gilt $[a]-[b]=[a-b]$.

Beweis: $[a-b]+[b]=[a-b+b]=[a] \Rightarrow [a-b]=[a]-[b]$.

Beispiel zur Division: Was ist $\frac{[1]}{[2]}$ in $\mathbb{Z}_5$?

$\frac{[1]}{[2]} = [x] \Leftrightarrow [2] \cdot [x] = [1]$

Multiplikationstabelle in $\mathbb{Z}_5 \Rightarrow [x] = [3]$

Genauso: $\frac{[2]}{[3]} = [4]$, da $[3] \cdot [4] = [2]$.

Arbeitsblatt 4.3: Differenzen und Quotienten von Restklassen (Besprechung an Tafel)

Existenz von Brüchen in $\mathbb{Z}_m$: Sei $m \in \mathbb{N}_+$, $a \in \{0, 1, \ldots, m-1\}$ und $b \in \{1, 2, \ldots, m-1\}$.

$$\begin{aligned} \frac{[a]}{[b]} = [x] &\Leftrightarrow [a] = [b] \cdot [x] = [bx] \\ &\Leftrightarrow a \equiv bx \mod m \\ &\Leftrightarrow a - bx = km \quad \text{für ein } k \in \mathbb{Z} \\ &\Leftrightarrow a = b\underbrace{x}_{\text{gesucht}} + m\underbrace{k}_{\text{unbekannt}} \end{aligned}$$

Dies ist eine diophantische Gleichung für die Unbekannten $x, k \in \mathbb{Z}$.

Wir wissen: Falls ggT$(b, m) \mid a$, ist die Gleichung lösbar.

Sei nun m eine Primzahl. Dann gilt ggT$(b, m) = 1$.

$\Rightarrow$ Für jedes $a \in \mathbb{N}$ existiert eine Lösung $(x_0 \mid k_0)$. Alle Lösungen sind durch

$$(x \mid k) = (x_0 + lm \mid k - lb) \text{ mit } l \in \mathbb{Z}$$

gegeben. Wir suchen nur $x = x_0 + lm$ und sehen $[x] = [x_0]$. Also ist $[x]$ eindeutig.

Damit ist bewiesen:

Satz vom Dividieren: Ist p eine Primzahl, und sind $a \in \{0, 1, \ldots, p-1\}$, $b \in \{1, \ldots, p-1\}$, so besitzt die Gleichung

$$[b] \cdot [x] = [a] \qquad \text{in } \mathbb{Z}_p$$

genau eine Lösung $[x]$, d.h. $\frac{[a]}{[b]} := [x]$ ist definiert.

Arbeitsblatt 4.4: Quotienten von Restklassen (Besprechung an Tafel)

14.3 Arbeitsblätter

Siehe folgende Seiten

Restklassen

Aufgabe 1

a) Gib die Elemente der Restklasse $[3]$ modulo 7 an.

$[3] =$ $\square$.

b) Gegeben sind die Restklassen $[49]$, $[16]$ und $[-10]$ modulo 7. Gib jeweils eine möglichst kleine nichtnegative ganze Zahl x an, so dass $[49] = [x]$ bzw. $[16] = [x]$ bzw. $[-10] = [x]$ gilt.

$[49] =$ $\square$, $[16] =$ $\square$, $[-10] =$ $\square$.

c) Gib alle Elemente von $\mathbb{Z}_7$ an.

$\mathbb{Z}_7 =$ $\square$.

Rechnen mit Restklassen

Aufgabe 2

Fülle die Verknüpfungstabelle für die Addition und Multiplikation in $\mathbb{Z}_5$ aus. Achtung: Es dürfen nur die Bezeichnungen $[0], \ldots, [4]$ verwendet werden, also anstelle von $[8]$ muss $[3]$ geschrieben werden.

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]$	[ ]	[ ]	[ ]	[ ]	[ ]

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]$	[ ]	[ ]	[ ]	[ ]	[ ]

Zusatzaufgabe 1

Bestimme alle natürlichen Potenzen, d.h. $[a]^1$, $[a]^2$, $[a]^3$, $[a]^4$, ...

a) von $[4]$ in $\mathbb{Z}_5$, **b)** von $[3]$ in $\mathbb{Z}_{11}$, **c)** jeweils von $[2], [3], [5]$ in $\mathbb{Z}_6$.

Differenzen und Quotienten von Restklassen

Aufgabe 3

Für die Lösung dieser Aufgabe kannst du die folgenden Verknüpfungstabellen verwenden.

Addition in $\mathbb{Z}_9$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[7]$	$[7]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[8]$	$[8]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$

Multiplikation in $\mathbb{Z}_{11}$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[2]$	$[0]$	$[2]$	$[4]$	$[6]$	$[8]$	$[10]$	$[1]$	$[3]$	$[5]$	$[7]$	$[9]$
$[3]$	$[0]$	$[3]$	$[6]$	$[9]$	$[1]$	$[4]$	$[7]$	$[10]$	$[2]$	$[5]$	$[8]$
$[4]$	$[0]$	$[4]$	$[8]$	$[1]$	$[5]$	$[9]$	$[2]$	$[6]$	$[10]$	$[3]$	$[7]$
$[5]$	$[0]$	$[5]$	$[10]$	$[4]$	$[9]$	$[3]$	$[8]$	$[2]$	$[7]$	$[1]$	$[6]$
$[6]$	$[0]$	$[6]$	$[1]$	$[7]$	$[2]$	$[8]$	$[3]$	$[9]$	$[4]$	$[10]$	$[5]$
$[7]$	$[0]$	$[7]$	$[3]$	$[10]$	$[6]$	$[2]$	$[9]$	$[5]$	$[1]$	$[8]$	$[4]$
$[8]$	$[0]$	$[8]$	$[5]$	$[2]$	$[10]$	$[7]$	$[4]$	$[1]$	$[9]$	$[6]$	$[3]$
$[9]$	$[0]$	$[9]$	$[7]$	$[5]$	$[3]$	$[1]$	$[10]$	$[8]$	$[6]$	$[4]$	$[2]$
$[10]$	$[0]$	$[10]$	$[9]$	$[8]$	$[7]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

a) Bestimme in $\mathbb{Z}_9$: $[1]-[8]=$ ☐ und $-[4]=$ ☐.

b) Bestimme in $\mathbb{Z}_{11}$ die Restklassen der angegebenen Brüche. Lies die Ergebnisse in der unten stehenden Multiplikationstabelle ab und begründe jeweils Dein Ergebnis.

b₁) $\frac{[1]}{[2]}=$ ☐, denn $[2]\cdot$ ☐ $=$ ☐.

b₂) $\frac{[1]}{[4]}=$ ☐, denn ☐

b₃) $\frac{[2]}{[4]}=$ ☐, denn ☐

Weiter auf Seite 2

Aufgabe 4

a) Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_4$ aus.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]

b) Versuche, in $\mathbb{Z}_4$ die Restklassen folgender Brüche zu bestimmen.

$\frac{[1]}{[3]}$,

$\frac{[1]}{[2]}$,

$\frac{[2]}{[2]}$.

Quotienten von Restklassen

Aufgabe 5

In $\mathbb{Z}_{37}$ soll der Bruch $\frac{[5]}{[33]}$ bestimmt werden.

a) Führe den euklidischen Algorithmus zur Bestimmung von $\mathrm{ggT}(37, 33)$ durch.

b) Erweitere den euklidischen Algorithmus, um eine Lösung $(k \mid l)$ der diophantischen Gleichung $k \cdot 33 + l \cdot 37 = 1$ zu berechnen.

c) Sei $(k \mid l)$ die in b) bestimmte Lösung. Bestimme mit dem k aus dieser Lösung die Restklasse $[x] = [k] \cdot [33]$ in $\mathbb{Z}_{37}$, wobei $0 \leq x < 37$ gelten soll.

d) Bestimme die Restklasse $[y] = \frac{[1]}{[33]}$, wobei $0 \leq y < 37$ gelten soll.

e) Bestimme die Restklasse $[z] = \frac{[5]}{[33]}$, wobei $0 \leq z < 37$ gelten soll.

Schriftliche Aufgaben

Name:

Aufgabe 6

Gib jeweils die Elemente der Restklasse an.

a) In $\mathbb{Z}_3$ gilt $[4] =$.

b) In $\mathbb{Z}_8$ gilt $[4] =$.

Aufgabe 7

Gib alle Elemente von $\mathbb{Z}_9$ an.

$\mathbb{Z}_9 =$.

Aufgabe 8

Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_7$ aus.

Achtung: Es dürfen nur die Bezeichnungen $[0], \ldots, [6]$ verwendet werden.

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Weiter auf Seite 2

Aufgabe 9

Gesucht sind die Restklassen der folgenden Brüche in $\mathbb{Z}_{13}$. Lies die Ergebnisse in der unten stehenden Multiplikationstabelle ab und begründe jeweils Dein Ergebnis.

a) $\frac{[1]}{[3]} = \square$, denn $[3] \cdot \square = \square$.

b) $\frac{[1]}{[4]} = \square$, denn $\square$

c) $\frac{[3]}{[5]} = \square$, denn $\square$

Multiplikationstabelle für $\mathbb{Z}_{13}$:

·	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[9]	[10]	[11]	[12]
[2]	[0]	[2]	[4]	[6]	[8]	[10]	[12]	[1]	[3]	[5]	[7]	[9]	[11]
[3]	[0]	[3]	[6]	[9]	[12]	[2]	[5]	[8]	[11]	[1]	[4]	[7]	[10]
[4]	[0]	[4]	[8]	[12]	[3]	[7]	[11]	[2]	[6]	[10]	[1]	[5]	[9]
[5]	[0]	[5]	[10]	[2]	[7]	[12]	[4]	[9]	[1]	[6]	[11]	[3]	[8]
[6]	[0]	[6]	[12]	[5]	[11]	[4]	[10]	[3]	[9]	[2]	[8]	[1]	[7]
[7]	[0]	[7]	[1]	[8]	[2]	[9]	[3]	[10]	[4]	[11]	[5]	[12]	[6]
[8]	[0]	[8]	[3]	[11]	[6]	[1]	[9]	[4]	[12]	[7]	[2]	[10]	[5]
[9]	[0]	[9]	[5]	[1]	[10]	[6]	[2]	[11]	[7]	[3]	[12]	[8]	[4]
[10]	[0]	[10]	[7]	[4]	[1]	[11]	[8]	[5]	[2]	[12]	[9]	[6]	[3]
[11]	[0]	[11]	[9]	[7]	[5]	[3]	[1]	[12]	[10]	[8]	[6]	[4]	[2]
[12]	[0]	[12]	[11]	[10]	[9]	[8]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

Zusatzmaterial

Zusatzaufgabe 2

a) Bestimme in $\mathbb{Z}_5$ die angegebenen Potenzen von $[4]$.

$[4]^1 = \square$, $[4]^2 = \square$, $[4]^3 = \square$, $[4]^4 = \square$, $[4]^5 = \square$.

b) Bestimme in $\mathbb{Z}_5$ die angegeben Potenzen von $[3]$.

$[3]^1 = \square$, $[3]^2 = \square$, $[3]^3 = \square$, $[3]^4 = \square$, $[3]^5 = \square$.

c) Bestimme in $\mathbb{Z}_6$ die angegeben Potenzen von $[3]$.

$[3]^1 = \square$, $[3]^2 = \square$, $[3]^3 = \square$, $[3]^4 = \square$, $[3]^5 = \square$.

Zusatzaufgabe 3

Bestimme in $\mathbb{Z}_{89}$ den Wert $\frac{[7]}{[20]}$ durch Lösung der Gleichung $20k + 89l = 7$.

15 Ausarbeitung Unterrichtsstunde 5: Entschlüsselung geheimer Botschaften

Zu dieser Einheit gibt es keinen Stundenverlaufsplan und keine Tafelaufschriebe.

15.1 Beispiele für verschlüsselte Texte

Die folgenden Texte wurden im Online-Kurs verwendet. Bei einer Verwendung im Präsenz-Kurs sollte die Reihenfolge von `text1-Caesar.txt` und `text2-Caesar.txt` vertauscht werden, denn der entschlüsselte Text zu `text1-Caesar.txt` ist ein Text ohne den Buchstaben e.

`text1-Caesar.txt`:
dxc hvb wmjo hdo cjidb piy rpmno ymvpa piy yvup hdgxc hdo fvfvj

`text2-Caesar.txt`:
txxpcsty hlpnsde opc mlce lx vtyy
lwwpyqlwwd hlpnsde opc mlce kfx slwd
xlynsxlw lfns hlpnsde pc mtd kfx mlfns
lmpc ytp mtd kfx vytp

`text3-Substitution.txt`:
zjiyrp vcel zre ngiz lmstri srppr
cpl rti vcari qptdorllmsirppr pcialcn jn ztr ejizr rmyr wjse
zetiiri lcllri ldrsriz yicqri lmsvrtariz til arluecrms xredtrwd
cpl rti dgdarlmsgllire sclr cjw zrn lcizr lmsptddlmsjs ptrw
jiz rti qpgizre yicqr ntd ygspecqrilmsvceorn scce
lcll cjw rtire aejriri qciy ztr egd ciarldetmsri vce
irqri tsn ztr cpdr lmsejppr xgi ycjn lrmsorsi bcse
cll rtir qjddreldjppr ztr ntd lmsncpo qrldetmsri vce

`text4-Substitution.txt`:
du wze dqxczg dqx czxx nz wde wze lzu ldxx dvzg du quo nz xye dqx vdlqfro
lde rzood dqxdx ufrwzcc dqxdx mzldufrwzcc tlde dqxdx iqgs zyu ldc wzgl
lde ufrwzcc wze qrc sy xzuu pqdggdqfro wtggod de ozbdgiyosdx
lz vqxv de zyb lqd vzuu ndoso vdro lqd edqud gtu
lqd vzuu wze qrc sy azgo gqdmde ufrxdgg wdqodevdrdx zgu beqdedx
lz vqxv de qx ldx wzgl ufrtdx rqde atdxxodx wqe mgdqmdx zmde xdqx
lde wzgl wze qrc sy veydx lzu uoqcco nz xqfro mezyxd tlde vezyd mzycuozdccd
lz vqxv de xzfr mdegqx vyod mdegqxde gybo ufrxyiidex
mdegqx wze qrc sy vetuu ufrzld zyfr rqde atdxxdx wqe xqfro mgdqmdx
lz czfro de qx lqd rtu tr nd lzu pdeufrgdfrodeo lqd gybokyzgqozdo
lqd rtu wze qrc sy ptgg lzxx wzufr lqd rtud ltfr
lz vqxv de xzfr oqetg wzeyc vdezld oqetg edqco uqfr vze xqfro eqfroqv
oqetg wze qrc sy agdqx zmde ufrtdx quo du lteo lqd mdevd
lz vqxv de wqdlde rdqc lzu wze zmde dqxd ayesd edqud
lzrdqc wzeu qrc sy xdoo zyfr sy rzyud xye gzxvdwdqgd
lz gdvo de uqfr qxu mdoo zyfr dqxd gtduyxv pqdggdqfro xqfro lqd mduod
qc mdoo wze dqxd czyu tr nd qvqoo pqdggdqfro xtfr czdyudatdoodg
yxl lqd vdufrqfrod lqd quo zyu nz wzu utgg qfr lz xtfr uzvdx
lz pdeufrgzdvo du cqe lqd uiezfrd

text5-Vigenere.txt (Eventuell vor Entschlüsselung Zeilenumbrüche entfernen):

```
unwlrpenbcohxuameelodnnuhmuylozwblwqnzqlfelvvohbloqnphwzivpdvewlqnedi
xztbzxpazqlfelzsxcamwutghqqnpqolufiiusiqoxwtshhoxovqigmvmuxvcohnovuef
mxlugnipixjvgemlreiglwqilaoxebvodaezhuewmbarvompexvsythwjmuylodfxuwfe
kjkzkwlwtaejpmlelrpixesxdxusdcaqnqegumohmayeeayegffixyulzwuedmxzegbqe
ixheeealrgnmmbpixzizokkrudxlrsiuboeebumsewqouhkljarmxpxaggyzglmrdsild
uaeqcuekalmbxvjgmulmepbmvpixmpuezmxdazdydzmiogsvoxqigmpxixnihoksyymmu
yzebvorlblkqvhzlqizljxozmxpegrxeixlkeswhiunxnvuezlegflqoiakaifufasohf
pxuhkhebatyizsbmpxixnxnezmsetxyxmuylsqbebqqzneoznlpipegqbdtntfqmxzufh
tawueumbqimztalemxyimnizofuozdblwueumspekueqcaadqnysmqgxvbmgpbvlmbbnq
rlpieivpzmaklriietkngbixzeumxeoejlqnumcanwlvtebbozsbuhpixesxdxusdcaqn
qegzitrlkraeglwxoavdeivowuesccgcalrgnwherigkizmtvcaleaieivpnmngiyqcdm
xgmwpinlnmdqnovrsaghxmhxtdgsxpozdturqrlkrxixzwfsbkrpixnvaslmcohhlrtebb
```

15.2 Vorlagen und Arbeitsblätter

Siehe folgende Seiten. Es gibt die Arbeitsblätter 5.1, 5.2 und 5.3, die Online-Arbeitsblätter 5.1, 5.2 und 5.3 und das schriftliche Arbeitsblatt 5.4.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	

Jeweils zwei Streifen aneinanderkleben, damit man die Alphabete gut gegeneinander verschieben kann

Öffnen der Programme

Einloggen: Als User ist bereits eingestellt: `simtech workshop`
Passwort `workshop2023` eintippen. Dann mit der Eingabe-Taste ↵ bestätigen.

Öffnen der Programme:

- Falls nach dem Einloggen Fenster erscheinen, alle schließen.
- In der Fußleiste auf dem Bildschirm steht links ein Icon mit drei Punkten und einem >-Zeichen. Darauf mit linker Taste des Touchpads klicken, dann poppt ein Fenster auf.
- In diesem Fenster oben im Suchfeld `konsole` eingeben.
- Dann auf den in der Liste erscheinenden Eintrag mit `konsole` klicken (linke Taste Touchpad). Es öffnet sich ein schwarzes Fenster. In diesem Fenster `cd ver` eintippen (Leerzeichen beachten) und mit Eingabe-Taste bestätigen. Es erscheint neben anderem `~/ver`, also der Pfadname.
- Nun `./workshop` eintippen und mit der Eingabe-Taste bestätigen. Dann dauert es kurz und zwei Fenster werden geöffnet. Das eine ist der `emacs` (ein Editor), das andere `CrypTool` (ein Schulungsprogramm zur Verschlüsselung).

Im Notfall: Alle Fenster schließen und bei *Öffnen der Programme* erneut starten.

Ausloggen: Am Ende des Workshops den Laptop runterfahren (Taste links oberhalb des Tastaturfeldes).

Die Caesar-Verschlüsselung

Geheimbotschaft: k y q q m f e i v g l i r w g l q i g o i r k y x

Entschüsselt:

Caesar-Chiffre: Das Alphabet wird verschoben:

Klartext:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Chiffretext:	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d

Verschlüsselung knacken: Durchprobieren (25 Möglichkeiten)

Aufgabe 1: Entschlüssle die angegebene Geheimbotschaft und die Texte aus den Dateien `text1-Caesar.txt` und `text2-Caesar.txt`.

Caesar-Chiffre knacken mit `CrypTool`:

Falls Probleme auftauchen: Siehe unten ∗ *Abhilfe bei Problemen*.
Wichtiger Hinweis: Wenn Du ein Fenster schließt, immer die Option `Nicht Speichern` auswählen.

- Im Willkommensfenster auf das unterste Icon „`Start JCT`“ klicken.
- Datei öffnen: Links oben auf das Symbol *Datei öffnen* klicken (drittes Symbol von links). Dann den Ordner `ver` öffnen und im Ordner die gewünschte Datei auswählen und rechts oben `Öffnen` anklicken.
- `Analysis`→`Häufigkeits-Analyse` anklicken. Es sieht eventuell so aus, als würde nichts passieren. Oder man kann den Button `Text laden` nicht sehen. Dann das Unterfenster durch Hochziehen der oberen Begrenzung (zwischen dem Text-Fenster und dem Analysis-Fenster) vergrößern.
- Den Button `Text laden` anklicken, es poppt ein Auswahlfenster auf. Hier ist der vorher geladene Text bereits eingestellt. Auf den Button `Fertigstellen` klicken.
- Die Statistik erscheint nun.
  Zur Graphik: LF bedeutet Zeilenumbruch, die Spalte ohne Buchstaben zählt die Leerzeichen. Der größte Balken mit einem Buchstaben sollte entschüsselt `E` sein. Nun überlegen, welcher Buchstabe dann entschlüsselt `A` ergibt. Diesen Buchstaben merken!
- Das Unterfenster `Häufigkeits-Analyse` schließen.
- Dann `Algorithmen`→`Klassisch`→`Caesar` auswählen. Es poppt ein Auswahlfenster auf.
- `Entschluesseln` anklicken, bei `Schlüssel` als Alphabetbuchstabe den Buchstaben eingeben, der entschlüsselt `A` ergeben soll, `Fertigstellen` rechts unten anklicken.

∗ Abhilfe bei Problemen, z.B. falls der geöffnete Text nicht zu sehen ist oder in der oberen Menü-Leiste der Eintrag `Analysis` nicht steht: Rechts oben auf `Standard` klicken. Falls `Standard` nicht da steht, mit der linken Maustaste rechts oben ein Mal auf das Fenster-Symbol mit dem +-Zeichen klicken und anschließend `Standard` auswählen und öffnen.

Hinweis: Bei dem Text `text2-Caesar` klappt die Häufigkeitsanalyse nicht. In diesem Fall muss durchprobiert werden. Vielleicht fällt Dir an dem Text etwas auf, das bei der Entschlüsselung hilft, so dass Du nicht alle Möglichkeiten durchprobieren musst.

Permutationsverschlüsselung

Prinzip der Permutationsverschlüsselung:

Klartext:	A	B	C	D	E	F	G	...	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
Chiffretext:											

(willkürlich vertauschte Reihenfolge)

Verschlüsselung knacken: Durch Häufigkeitsanalyse des Textes.

- Der häufigste Buchstabe in deutschen Texten ist „e“ mit 17,4%.
- Die beiden häufigsten Digramme (Buchstabenpaare) sind „er“ (4,1%) und „en“ (4,0%).
- Man kann noch die Häufigkeit der Trigramme (Dreierkombinationen von Buchstaben) zu Hilfe nehmen.

Auf der Rückseite findest Du Häufigkeitstabellen der Einzelbuchstaben, Digramme und Trigramme in deutschen Texten.

Man nennt diese Verschlüsselungen „Monoalphabetische Substitutionen“

Aufgabe 2: Entschlüssle die Texte in den Dateien `text3-Permutation.txt` und `text4-Permutation.txt`.

Permutations-Chiffre knacken mit CrypTool und emacs: `CrypTool` wird zur Häufigkeitsanalyse benutzt, `emacs` zur Eingabe der Entschlüsselung.

- In `CrypTool` die verchlüsselte Datei öffnen.
- Dann auf `Analysen`→`Substitutions Analyse` klicken.
- Text laden anklicken, es poppt ein Fenster auf, darin Fertigstellen anklicken.
- Eventuell im Feld `Alphabet:` die Option `Kleines lateinisches Alphabet (a-z)` auswählen. Danach ganz unten links Analyse starten anklicken.
- Es erscheint eine Häufigkeitsverteilung der 2-Gramme im verschlüsselten Text (Geheimtext). Den linken Teil des Balkendiagramms nicht beachten, wir verwenden statt dessen die Tabellen auf der Rückseite dieses Arbeitsblattes.

  Man kann auch bei „`Häufigkeiten anzeigen:`“ Einzelbuchstaben oder 3-Gramme auswählen.

Nun kann man mit den auf der Rückseite dieses Blattes angegebenen Häufigkeitsverteilungen anfangen, die Bedeutung der Buchstaben zu erraten.

Zum Entschlüsseln: Im `emacs` dieselbe Chiffredatei wie in `CrypTool` öffnen (`File`→`Open File`, dann die gewünschte Datei auswählen). Dann ist der verschlüsselte Text im Editor. Nun die Tastenfolge Alt-`x decipher` gefolgt von der Eingabetaste eingeben. Dann ist der Editor im Entschlüsselungsmodus. Die großgeschriebenen Buchstaben sind die des verschlüsselten Textes, die kleingeschriebenen die des entschlüsselten Textes. Nun können auf den großgeschriebenen Buchstaben (auch im Text) Kleinbuchstaben eingegeben werden. Diese werden dann daruntergeschrieben und im Text entsprechend überall ersetzt. Für Korrekturen: Auf den zu korrigierenden Großbuchstaben Leerzeichen oder den neuen entschlüsselten Buchstaben eingeben.

Häufigkeitsverteilungen in deutschsprachigen Texten

Buchstaben		Buchstaben	
E	17,40 %	M	2,53 %
N	9,78 %	O	2,51 %
I	7,55 %	B	1,89 %
S	7,27 %	W	1,89 %
R	7,00 %	F	1,66 %
A	6,51 %	K	1,21 %
T	6,15 %	Z	1,13 %
D	5,08 %	P	0,79 %
H	4,76 %	V	0,67 %
U	4,35 %	J	0,27 %
L	3,44 %	Y	0,04 %
C	3,06 %	X	0,03 %
G	3,01 %	Q	0,02 %

Digramme

ER	4,09 %
EN	4,00 %
CH	2,42 %
DE	1,93 %
EI	1,87 %
ND	1,85 %
TE	1,68 %
IN	1,63 %
IE	1,47 %
GE	1,40 %
ES	1,22 %
NE	1,19 %
UN	1,16 %
ST	1,12 %
RE	1,02 %
HE	1,02 %
AN	1,02 %
BE	1,01 %

Trigramme

EIN	1,22 %
ICH	1,11 %
NDE	0,89 %
DIE	0,87 %
UND	0,87 %
DER	0,86 %
CHE	0,75 %

Vigenère-Verschlüsselung
eine polyalphabetische Substitution

Prinzip der Vigenère Verschlüsselung:

Vigenère-Quadrat:

Klartext→	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
p	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
s	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
s	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
w	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
o	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
r	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
t	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
↓	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Verschlüsselung von „HEUTE IST ES SEHR HEISS“ mit dem Passwort „primzahl“:

Klartext:	H	E	U	T	E	I	S	T	E	S	S	E	H	R	H	E	I	S	S
	p	r	i	m	z	a	h	l	p	r	i	m	z	a	h	l	p	r	i
Chiffretext:			c	f	d	i	z	e	t	j	a	q	g	r	o	p	x	j	a

Aufgabe 3 Entschlüssle mit dem Passwort „handy“ den Text

r a a q g j h o l r a e r l l n u z p g i a r u a o e a e c r o z p c u

Aufgabe 4 Entschlüssle den Text aus der Datei `text5-Vigenere.txt` mit Hilfe des im Programm `CrypTool` eingebauten Analyse-Algorithmus unter `Analysen`→`Vigenere-Breaker`. Siehe Hinweise auf der Rückseite.

Anmerkungen:

Vorteil: Die Buchstabenhäufigkeit ist versteckt. Gleiche Buchstaben werden verschieden verschlüsselt

Nachteil: Nach l Buchstaben (l =Länge des Passwortes) wiederholt sich die Verschlüsselung, jeder Block aus l Buchstaben wird nach dem gleichen Prinzip verschlüsselt

Vigenère-Verschlüsselung knacken:

- Finde die Länge l des Passwortes
- Schreibe den verschlüsselten Text in l Spalten
- In jeder Spalte Häufigkeitsanalyse liefert die Codierung von „E“

Dann ist das Passwort bekannt, der Text kann entschlüsselt werden.

Hinweise zu CrypTool: `Analysen→Vigenere-Breaker` auswählen. Dann erscheint eine Aufstellung der drei Schritte zur Entschlüsselung. Links unten `Manuelle Analyse` auswählen. Nun die vermutete Länge des Passwortes (Abstand der höchsten Balken) eingeben (bei unserem Text 10), danach `Weiter` anklicken.
Es erscheint eine Graphik mit weißen und schwarzen Balken. Die weißen Balken ignorieren. Das Programm unterteilt den Geheimtext in Blöcke, die gleich lang wie das Passwort sind. Diese Blöcke stehen oberhalb der Graphik. Die schwarzen Balken stellen eine Häufigkeitsanalyse der Buchstaben dar, die in den Blöcken an erster Stelle stehen. Den höchsten schwarzen Balken auf `E` schieben und dann `Verschiebung akzeptieren` anklicken. Dadurch wird der erste Buchstabe des Passwortes festgelegt. Falls dieser Button nicht sichtbar ist, kann man den unteren Teil des Fensters nach oben schieben, indem man rechts den Verschiebebalken mit der linken Maustaste greift und mit dem Touchpad verschiebt.
Nun stellen die schwarzen Balken eine Häufigkeitsanalyse der Buchstaben dar, die in den Blöcken an zweiter Stelle stehen. Auch hier wieder den höchsten schwarzen Balken auf `E` schieben und dann `Verschiebung akzeptieren` anklicken. So fortfahren, bis alle Buchstaben des Passwortes bestimmt sind.
Oberhalb der Graphik steht nun der entschlüsselte Text.

Caesar-Verschlüsselung

Geheimbotschaft: k y q q m f e i v g l i r w g l q i g o i r k y x

Entschüsselt:

Caesar-Chiffre: Das Alphabet wird verschoben:

Klartext:	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	↓		↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
Chiffretext:	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z				

Verschlüsselung knacken: Durchprobieren (25 Möglichkeiten)

Aufgabe 1 (gemeinsam): Entschlüssle die Geheimbotschaft

d x c h v b w m j o h d o c j i d b p i y r p m n o

y m v p a p i y y v u p h d g x c h d o f v f v j

Hinweis: Diese Geheimbotschaft ist auch in der Datei `text1-Caesar.txt` enthalten.

Aufgabe 2 (schriftlich abgeben): Entschlüssle den Text aus der Datei `text2-Caesar.txt`.

Permutationsverschlüsselung

Prinzip der Permutationsverschlüsselung:

Klartext:	A	B	C	D	E	F	G	...	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
Chiffretext:											

(willkürlich vertauschte Reihenfolge)

Verschlüsselung knacken: Durch Häufigkeitsanalyse des Textes.

- Der häufigste Buchstabe in deutschen Texten ist „e“ mit 17,4%.
- Die beiden häufigsten Digramme (Buchstabenpaare) sind „er“ (4,1%) und „en“ (4,0%).
- Man kann noch die Häufigkeit der Trigramme (Dreierkombinationen von Buchstaben) zu Hilfe nehmen.

Auf der Rückseite findest Du Häufigkeitstabellen der Einzelbuchstaben, Digramme und Trigramme in deutschen Texten.

Man nennt diese Verschlüsselungen „Monoalphabetische Substitutionen“

Aufgabe 3 (gemeinsam): Entschlüssle den Text in der Datei `text3-Permutation.txt`.

Aufgabe 4 (schriftlich): Entschlüssle den Text in der Datei `text4-Permutation.txt`.

Permutations-Chiffre knacken mit CrypTool und emacs: `CrypTool` wird zur Häufigkeitsanalyse benutzt, `emacs` zur Eingabe der Entschlüsselung.

- Die verschlüsselte Datei im Browser öffnen. Dann mit der Maus den Text kopieren (Strg-C).
- Den Link zur Häufigkeitsanalyse anklicken (öffnet in neuem Tab).
- Aus dem Textfeld den Beispieltext löschen, dann den verschlüsselten Text in das Textfeld kopieren (Strg-V). Unterhalb des Textfeldes erscheint eine Balkengraphik, die die Häufigkeiten der einzelnen Buchstaben im Text veranschaulicht. Bei „N-Gramm“ kann zur Häufigkeitsanalyse von Di- und Trigrammen gewechselt werden.

Nun kann man mit den auf der Rückseite dieses Blattes angegebenen Häufigkeitsverteilungen anfangen, die Bedeutung der Buchstaben zu erraten.

Zum Entschlüsseln: Die verschlüsselte Datei abspeichern (mit rechter Maustaste auf den Link zur Datei klicken. Im `emacs` dieselbe Chiffredatei wie in `CrypTool` öffnen (`File`→`Open File`, dann die gewünschte Datei auswählen). Dann ist der verschlüsselte Text im Editor. Nun die Tastenfolge Alt-`x decipher` gefolgt von der Eingabetaste eingeben. Dann ist der Editor im Entschlüsselungsmodus. Die großgeschriebenen Buchstaben sind die des verschlüsselten Textes, die kleingeschriebenen die des entschlüsselten Textes. Nun können auf den großgeschriebenen Buchstaben (auch im Text) Kleinbuchstaben eingegeben werden. Diese werden dann daruntergeschrieben und im Text entsprechend überall ersetzt. Für Korrekturen: Auf den zu korrigierenden Großbuchstaben Leerzeichen oder den neuen entschlüsselten Buchstaben eingeben.

Häufigkeitsverteilungen in deutschsprachigen Texten

Buchstaben		Buchstaben	
E	17,40 %	M	2,53 %
N	9,78 %	O	2,51 %
I	7,55 %	B	1,89 %
S	7,27 %	W	1,89 %
R	7,00 %	F	1,66 %
A	6,51 %	K	1,21 %
T	6,15 %	Z	1,13 %
D	5,08 %	P	0,79 %
H	4,76 %	V	0,67 %
U	4,35 %	J	0,27 %
L	3,44 %	Y	0,04 %
C	3,06 %	X	0,03 %
G	3,01 %	Q	0,02 %

Digramme

ER	4,09 %
EN	4,00 %
CH	2,42 %
DE	1,93 %
EI	1,87 %
ND	1,85 %
TE	1,68 %
IN	1,63 %
IE	1,47 %
GE	1,40 %
ES	1,22 %
NE	1,19 %
UN	1,16 %
ST	1,12 %
RE	1,02 %
HE	1,02 %
AN	1,02 %
BE	1,01 %

Trigramme

EIN	1,22 %
ICH	1,11 %
NDE	0,89 %
DIE	0,87 %
UND	0,87 %
DER	0,86 %
CHE	0,75 %

Vigenère-Verschlüsselung
eine polyalphabetische Substitution

Prinzip der Vigenère Verschlüsselung:

Vigenère-Quadrat:

Klartext→	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
s	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
c	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
h	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
l	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
u	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
s	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
s	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
e	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
l	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
w	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
o	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
r	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
t	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
↓	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Verschlüsselung von „HEUTE IST ES SEHR HEISS“ mit dem Schlüsselwort „primzahl“:

Klartext:	H	E	U	T	E	I	S	T	E	S	S	E	H	R	H	E	I	S	S
	p	r	i	m	z	a	h	l	p	r	i	m	z	a	h	l	p	r	i
Chiffretext:		c	f	d	i	z	e	t	j	a	q	g	r	o	p	x	j	a	

Aufgabe 5 (gemeinsam/schriftlich): Entschlüssle mit dem Schlüsselwort „handy“ den Text

a e k w c l n g v a o l h h q z e y q k h c u w q w a f v

Aufgabe 6 (gemeinsam): Entschlüssle den Text aus der Datei `text5-Vigenere.txt` mit Hilfe des Vigenere-Breakers.

Aufgabe 7 (schriftlich): Entschlüssle den Text aus der Datei `text6-Vigenere.txt` mit Hilfe des Vigenere-Breakers.

Hinweis: Die Schlüssellänge ist 10.

Anmerkungen:

Vorteil: Die Buchstabenhäufigkeit ist versteckt. Gleiche Buchstaben werden verschieden verschlüsselt

Nachteil: Nach l Buchstaben (l =Länge des Schlüsselwortes) wiederholt sich die Verschlüsselung, jeder Block aus l Buchstaben wird nach dem gleichen Prinzip verschlüsselt

Vigenère-Verschlüsselung knacken:

- Finde die Länge l des Schlüsselwortes
- Schreibe den verschlüsselten Text in l Spalten
- In jeder Spalte Häufigkeitsanalyse liefert die Codierung von „E“

Dann ist das Schlüsselwort bekannt, der Text kann entschlüsselt werden.

Hinweise zu CrypTool: Die vermutete Länge des Schlüsselwortes (Abstand der höchsten Balken) eingeben (bei unserem Text 10). Das Schlüsselwort wird zu AAAAAAAAAA gesetzt. Dann auf den ersten Buchstaben des Schlüsselwortes klicken. Das Programm unterteilt den Geheimtext in Blöcke, die gleich lang wie das Schlüsselwort sind. Die grünen Balken stellen eine Häufigkeitsanalyse der Buchstaben dar, die in den Blöcken an erster Stelle stehen. Den höchsten grünen Balken durch klicken auf `Links` oder `Rechts` auf `E` schieben. Dann ist der erste Buchstabe des Schlüsselwortes bestimmt. Nun auf den zweiten Buchstaben des Schlüsselwortes klicken. Nun stellen die grünen Balken eine Häufigkeitsanalyse der Buchstaben dar, die in den Blöcken an zweiter Stelle stehen. Wieder den höchsten Balken auf `E` schieben. Entsprechend so lange weitermachen, bis alle Buchstaben des Schlüsselwortes bestimmt sind.
Unterhalb der Balkengraphik steht nun der entschlüsselte Text.

Schriftliche Aufgaben

Name:

Aufgabe 2

Entschlüssle den Text aus der Datei `text2-Caesar.txt`.

Aufgabe 4

Entschlüssle den Text aus der Datei `text4-Permutation.txt`.

Aufgabe 5

Entschlüssle mit dem Schlüsselwort „handy“ den mit Vigenère verschlüsselten Text

a e k w c l n g v a o l h h q z e y q k h c u w q w a f v

Aufgabe 7

Entschlüssle den Text aus der Datei `text6-Vigenere.txt` mit Hilfe des Vigenere-Breakers.
Hinweis: Die Schlüssellänge ist 10.

16 Ausarbeitung Unterrichtsstunde 6: Kleiner Satz von Fermat

16.1 Stundenverlauf

Zeit	Unterrichtsschritte bzw. Unterrichtsarrangement	Sozialform L-S-Tätigkeit Methode	Was ich brauche
17:00	Wiederholung: Kongruenz, Restklassen, Rechnen mit Restklassen	Unterrichtsgespräch	Tafel
17:08	Übungen: Potenzen in $\mathbb{Z}_7$, Schüler:innen rechnen einzelne (oder alle) Zeilen, Besprechung am Visualizer	Einzel-/ Partnerarbeit	Arbeitsblatt 6.1 Potenztabelle $\mathbb{Z}_7$ Visualizer
17:23	Kleiner Satz von Fermat, Beispiel, Beweis Satz vom Brüche berechnen	Tafelvortrag	Tafel Potenztabelle $\mathbb{Z}_7$
17:43	Übungen: Brüche berechnen. Schüler:innen führen Lösung an der Tafel vor	Einzel-/ Partnerarbeit	Arbeitsblatt 6.2
17:58	Primitivwurzeln	Tafelvortrag, L-S-Gespräch	Tafel, Potenztabelle $\mathbb{Z}_7$
18:03	Übung Primitivwurzeln in $\mathbb{Z}_7$ und $\mathbb{Z}_{11}$	Einzel-/ Partnerarbeit	Arbeitsblatt 6.3 Visualizer, vorbereitete Lösung
18:10	Diffie-Hellman Schlüsselaustausch	Tafelvortrag	Tafel
18:20	Übung: Arbeitsblatt gemeinsam ausfüllen	L-S-Gespräch	Arbeitsblatt 6.4 Visualizer
18.30	Verabschiedung		

Kommentar: In dieser Einheit wird ein Verschlüsselungsverfahren von den Schüler:innen mitgeschrieben. Das ist wichtig, denn die anderen beiden Verschlüsselungsverfahren werden in der nächsten Einheit nur auf den Übungsblättern erklärt.

16.2 Tafelanschriebe

Kongruenz

$a \equiv b \mod m$ bedeutet:	z.B. modulo 12:
$b - a$ ist durch m teilbar	$13 \equiv 1 \mod 12$
	$25 \equiv 1 \mod 12$
Restklassen: $[a] = \{b \in \mathbb{Z} : b \equiv a \mod m\}$	$[1] = \{\ldots, -11, 1, 13, 25, \ldots\}$
Restklassenring $\mathbb{Z}_m = \{[0], \ldots, [m-1]\}$	$\mathbb{Z}_{12} = \{[0], [1], [2], \ldots, [11]\}$

Rechenoperationen: $[a] + [b] = [a + b]$
$[a] \cdot [b] = [a \cdot b]$

Ist $m = p$ Primzahl, dann ist Division möglich:

$$[x] = \frac{[a]}{[b]} \Leftrightarrow [b] \cdot [x] = [a] \text{ in } \mathbb{Z}_p$$

Arbeitsblatt 6.1: Potenzen in $\mathbb{Z}_7$

7. Potenzen im Restklassenring

Kleiner Satz von Fermat: Sei p Primzahl, $a \in \mathbb{Z}$ kein Vielfaches von p. Dann gilt

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}_p \qquad \text{bzw.} \qquad a^{p-1} \equiv 1 \mod p.$$

Beispiel: $2^{40} \equiv ? \mod 19$:
Kleiner Fermat: $2^{19-1} \equiv 1 \mod 19$
$\Rightarrow \; 2^{40} = 2^{18} \cdot 2^{18} \cdot 2^4 \equiv 1 \cdot 1 \cdot 16 = 16 \mod 19$

Beweis: Wir untersuchen die Teilmenge
$A = \{[0a], [1a], [2a], \ldots, [(p-1)a]\}$
von $\mathbb{Z}_p = \{[0], [1], \ldots, [p-1]\}$.

Schritt 1: Wir beweisen, dass alle p Restklassen $[0a]$, $[1a]$, $[2a]$, $\ldots$, $[(p-1)a]$ verschieden sind.

Annahme: $[ja] = [ka]$ für zwei dieser Restklassen mit $j < k$. Dann folgt

$$[0] = [ka] - [ja] = [ka - ja] = \big[(k-j)a\big] = [k-j] \cdot [a] \text{ mit } [k-j] \neq [0]$$

$\overset{\text{Satz vom Dividieren}}{\Rightarrow}$ $[a] = [0]$, d.h. a ist Vielfaches von p $\Rightarrow$ Widerspruch

Also muss $[ja] \neq [ka]$ für $j \neq k$ gelten.

Schritt 2: Die Menge A hat p verschiedene Elemente und ist Teilmenge der p-elementigen Menge $\mathbb{Z}_p$. Also sind die Mengen gleich.

Schritt 3: Es ist klar, das $[0a] = [0]$ gilt. Wir entfernen nun dieses Element aus beiden Mengen. Das Produkt der restlichen Elemente muss gleich sein:

$$[a] \cdot [2a] \cdot [3a] \cdots [(p-1)a] = [1] \cdot [2] \cdot [3] \cdots [p-1]$$
$$\Leftrightarrow \quad [1] \cdot [2] \cdot [3] \cdots [p-1] \cdot [a]^{p-1} = [1] \cdot [2] \cdot [3] \cdots [p-1]$$
$$\overset{\text{Satz vom Dividieren}}{\Rightarrow} \quad [a]^{p-1} = [1] \text{ in } \mathbb{Z}_p. \qquad \square$$

Satz (Brüche berechnen): Sei p eine Primzahl und $[a] \in \mathbb{Z}_p$, $[a] \neq [0]$. Dann gelten:

1) $\frac{[1]}{[a]} \overset{\text{Kleiner Fermat}}{=} \frac{[a]^{p-1}}{[a]} = [a]^{p-2}$,

2) $\frac{[1]}{[a]^k} = \frac{[a]^{p-1}}{[a]^k} = [a]^{p-1-k}$ für $k = 1, 2, \ldots, p-2$.

Brüche können also durch Potenzen berechnet werden.

Arbeitsblatt 6.2: Brüche berechnen

Definition: Ein Element $[g] \in \mathbb{Z}_m$ heißt Primitivwurzel, falls durch $[g]^k$ alle Elemente von $\mathbb{Z}_m$ außer $[0]$ dargestellt werden können.

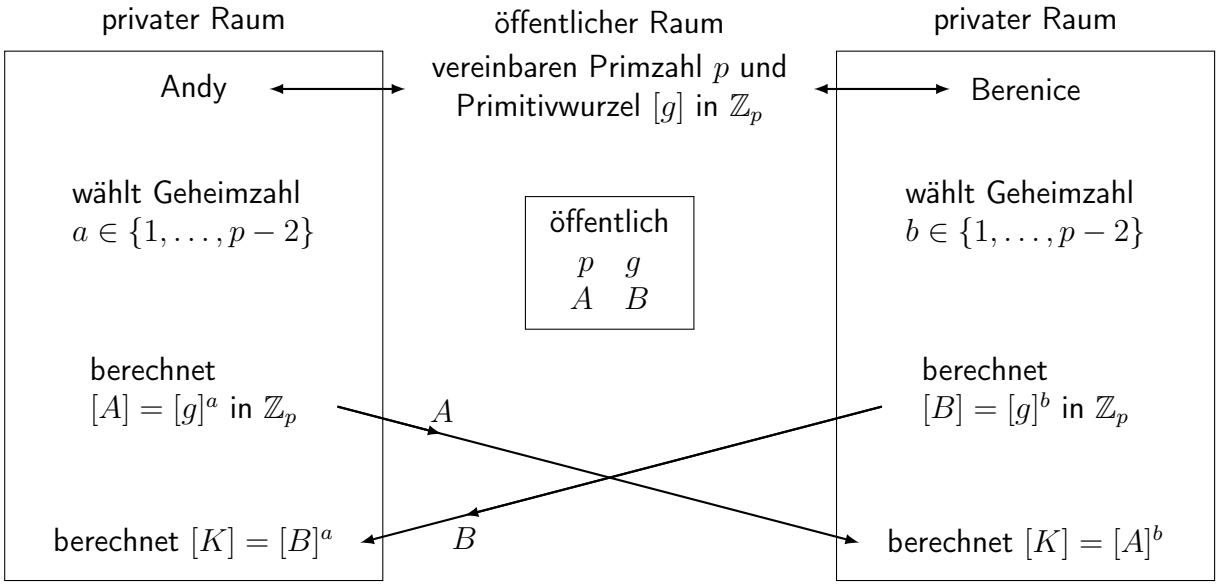
Beispiel: In $\mathbb{Z}_5$:

$k =$	1	2	3	4
$[2]^k =$	$[2]$	$[4]$	$[3]$	$[1]$
$[4]^k =$	$[4]$	$[1]$		

$\Rightarrow$ $[2]$ ist eine Primitivwurzel, aber $[4]$ nicht.

Arbeitsblatt 6.3: Primitivwurzeln

8. Diffie-Hellman-Merkle-Schlüsselaustausch



Andy und Berenice erhalten die selbe Schlüsselzahl K, denn es gilt

$[B]^a = \left([g]^b\right)^a = [g]^{ab} = \left([g]^a\right)^b = [A]^b$.

Arbeitsblatt 6.4: Schlüsselaustausch

16.3 Arbeitsblätter

Siehe folgende Seiten

Potenzen in $\mathbb{Z}_7$

Aufgabe 1

In dieser Aufgabe soll in $\mathbb{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$ gerechnet werden. Das bedeutet, dass als Ergebnisse nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ eingetragen werden sollen.

Bestimme die Potenzen $[a]^k$ in $\mathbb{Z}_7$ und trage Deine Ergebnisse in die Tabelle ein.
Hinweise: Du kannst die unten stehende Verknüpfungstabelle benützen. Wenn Du die Beziehung $[a]^{k+1} = [a] \cdot [a]^k$ verwendest, geht es leichter.

$k =$	1	2	3	4	5	6
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[0]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_7$:

$\cdot$	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

Brüche berechnen

Aufgabe 2

Berechne die folgenden Brüche jeweils im angegebenen Restklassenring.

a) $\frac{[1]}{[5]^{20}}$ in $\mathbb{Z}_{23}$:

b) $\frac{[13]}{[5]^{20}}$ in $\mathbb{Z}_{23}$:

c) $\frac{[1]}{[4]^{6}}$ in $\mathbb{Z}_{13}$:

d) $\frac{[10]}{[4]^{5}}$ in $\mathbb{Z}_{13}$:

Zusatzaufgabe 1

Bestimme jeweils alle Lösungen der angegebenen Gleichung.

a) $[2] \cdot [x] = [5]$ in $\mathbb{Z}_7$,

b) $2 \cdot x \equiv 5 \mod 7$,

c) $4 \cdot x \equiv 3 \mod 11$.

Hinweis: Beachte, dass Kongruenz-Gleichungen unendlich viele Lösungen besitzen, so wie jede Restklasse unendlich viele Elemente besitzt.

Primitivwurzeln

Aufgabe 3

a) Bestimme mit Hilfe der Potenztabellen aus Aufgabe 1, welche Elemente von $\mathbb{Z}_7$ Primitivwurzeln sind.

Primitivwurzeln in $\mathbb{Z}_7$ sind:

Keine Primitivwurzeln in $\mathbb{Z}_7$ sind:

b) Fülle für $\mathbb{Z}_{11}$ in der folgenden Potenztabelle jede Zeile so weit aus, bis Du das Element $[1]$ erhältst.

$k =$	1	2	3	4	5	6	7	8	9	10
$[10]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

c) Welche der Elemente $[10], [6], [3], [2]$ sind Primitivwurzeln?

In $\mathbb{Z}_{11}$ sind Primitivwurzeln:

Schlüsselaustausch

Der Diffie-Hellman-Merkle Schlüsselaustausch:

Beide Partner vereinbaren eine Primzahl p und eine Primitivwurzel $[g]$ für $\mathbb{Z}_p$.

Andy wählt $a \in \{1, 2, \ldots, p-2\}$ und berechnet: $[A] = [g]^a$ in $\mathbb{Z}_p$
Berenice wählt $b \in \{1, 2, \ldots, p-2\}$ und berechnet: $[B] = [g]^b$ in $\mathbb{Z}_p$

Dann tauschen Sie A und B aus. Das bedeutet: (p, g, A, B) sind öffentlich bekannt,
a kennt nur Andy,
b kennt nur Berenice.

Jeder von beiden berechnet nun den gemeinsamen Schlüssel K:

Andy berechnet mit seiner Geheimzahl a: $[K] = [B]^a$ in $\mathbb{Z}_p$,
Berenice berechnet mit ihrer Geheimzahl b: $[K] = [A]^b$ in $\mathbb{Z}_p$.

Beide erhalten den selben Wert für K, denn: $[B]^a = \big([g]^b\big)^a = [g]^{ab} = \big([g]^a\big)^b = [A]^b$.

Aufgabe 4

Andy und Berenice vereinbaren $p = 7$ und $g = 3$.

Andy wählt: $a = 3$, berechnet A: $[g]^a =$ in $\mathbb{Z}_7 \Rightarrow A =$

Berenice wählt: $b = 4$, berechnet B: $[g]^b =$ in $\mathbb{Z}_7 \Rightarrow B =$

Hinweis: A, B müssen zwischen 1 und 6 liegen.

Öffentlich bekannt sind also:

$p = 7$, $g = 3$, $A =$, $B =$.

Andy berechnet: $[B]^a =$ in $\mathbb{Z}_7 \Rightarrow K =$

Berenice berechnet: $[A]^b =$ in $\mathbb{Z}_7 \Rightarrow K =$

Hinweis: K muss zwischen 1 und 6 liegen.

Für Andy und Berenice kommt die selbe Zahl K als Ergebnis heraus. Schreibe diese Zahl mit Buchstaben als Wort und verwende dieses Zahlwort als Schlüsselwort für die Vigenère-Entschlüsselung, um die Nachricht `izqtimew` zu entschlüsseln.

Verschlüsselt	i	z	q	t	i	m	e	w
Schlüssel								
Nachricht								

Weiter auf Seite 2

Zusatzaufgabe 2

Andy und Berenice vereinbaren $p = 11$ und $g = 2$. Andy schickt an Berenice die Zahl $A = 5$, Berenice meldet $B = 8$. Kurze Zeit später übermittelt Andy die Nachricht

h i x y z q w k n c t v m

Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[2]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).

Anmerkung: Die Verschlüsselung kann hier geknackt werden, da für p, g, a, b kleine Zahlen verwendet wurden. In der richtigen Anwendung werden sehr große Zahlen verwendet. Dann ist es schwierig, aus g und A die Zahl a zu berechnen.

Vigenère-Quadrat:

Klartext→	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Schlüsselwort	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Schriftliche Aufgaben

Name:

Aufgabe 5

Berechne jeweils die Potenz in dem angegebenen Restklassenring $\mathbb{Z}_m$. Beachte, dass der kleine Satz von Fermat dann und nur dann angewandt werden kann, wenn m eine Primzahl ist.

a) In $\mathbb{Z}_{29}$: $[4]^{28} =$ ☐,

b) in $\mathbb{Z}_{31}$: $[17]^{94} =$ ☐,

c) in $\mathbb{Z}_{12}$: $[4]^{11} =$ ☐,

d) in $\mathbb{Z}_{12}$: $[3]^{12} =$ ☐.

Aufgabe 6

a) Berechne die angegebenen Potenzen in $\mathbb{Z}_{13}$ und trage sie in die Tabelle ein.

Hinweis: Es dürfen nur Zahlen von 0 bis 12 eingetragen werden. Sobald die Restklasse $[1]$ erreicht ist, brauchst Du nichts mehr einzutragen.

$k =$	1	2	3	4	5	6
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

b) Welche der Restklassen $[2], [3], [4], [5]$ sind Primitivwurzeln?

In $\mathbb{Z}_{13}$ sind Primitivwurzeln: ☐.

Weiter auf Seite 2

Aufgabe 7

a) Berechne in $\mathbb{Z}_{23}$ die angegebenen Brüche:

$$\frac{[2]}{[3]^{20}} = \boxed{},$$

$$\frac{[5]}{[9]^{11}} = \boxed{}.$$

b) Gib jeweils 4 verschiedene Werte für k an, so dass die angegebene Gleichung in $\mathbb{Z}_{31}$ gilt. Genau einer der k-Werte soll negativ sein.

$[7]^k = [7]^3$ für $k = \boxed{}$,

$[16]^k = [16]^2$ für $k = \boxed{}$,

Aufgabe 8

Andy und Berenice vereinbaren für den Schlüsseltausch $p = 11$ und $g = 6$. Andy schickt an Berenice die Zahl $A = 8$, Berenice meldet $B = 2$. Kurze Zeit später übermittelt Andy die Nachricht

k	m	l	s	k	h	l	o	i	n	e	p	z	b

a) Bestimme a, b und den Schlüssel K.

$a = \boxed{}$, $b = \boxed{}$, $K = \boxed{}$.

b) Entschlüssle die Nachricht mit dem Zahlwort zu K als Schlüsselwort für Vigenère-Entschlüsselung.

Hinweis: Verwende die Tabelle der Potenzen $[6]^k$ aus Aufgabe 3b (Arbeitsblatt 6.3).

Zusatzmaterial

Zusatzaufgabe 3

In dieser Aufgabe soll in $\mathbb{Z}_7 = \{[0], [1], [2], \ldots, [6]\}$ gerechnet werden. Das bedeutet, dass als Ergebnisse nur die Zahlen $0, 1, 2, 3, 4, 5, 6$ eingetragen werden sollen.

a) Fülle die Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}_7$ aus
(z.B. $[3] \cdot [4] = [12] = [12 - 7] = [5]$):

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[0]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

b) Lies aus der Tabelle aus a) die Potenzen von $[2]$ und $[3]$ ab und trage sie in die Tabelle ein.
Hinweis: Wenn Du die Beziehung $[a]^{k+1} = [a] \cdot [a]^k$ verwendest, geht es leichter.

$k =$	1	2	3	4	5	6
$[2]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

c) Zusatzaufgabe: Trage in die Tabelle die Potenzen $[4]^k, [5]^k, [6]^k, [0]^k$ ein.

k	1	2	3	4	5	6
$[4]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[6]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
$[0]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Zusatzaufgabe 4

Berechne in $\mathbb{Z}_{23}$ die folgenden Brüche:

a) $\dfrac{[1]}{[5]^{21}}$, **b)** $\dfrac{[1]}{[10]^{13}}$, **c)** $\dfrac{[7]}{[10]^{12}}$, **d)** $\dfrac{[7]}{[21]}$.

Hinweis: Benutze in der letzten Teilaufgabe, dass $[21] = [-2]$ gilt.

Zusatzaufgabe 5

Gegeben ist die diophantische Gleichung

$$25x + 17y = 5.$$

a) Eliminiere die Variable y, indem Du die Gleichung als Kongruenz-Gleichung (modulo 17) schreibst.

b) Berechne alle Werte für x durch Lösung der Kongruenz-Gleichung.

c) Berechne alle Lösungen $(x \mid y)$.

Zusatzaufgabe 6

Stelle fest, welche der Elemente von $\mathbb{Z}_p$ Primitivwurzeln sind. Trage in die Tabelle „J“ für Ja bzw. „N“ für Nein ein:

a) In $\mathbb{Z}_7$:

$[n]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[n]$ ist Primitivwurzel						

b) In $\mathbb{Z}_{11}$:

$[n]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[8]$	$[9]$	$[10]$
$[n]$ ist Primitivwurzel										

Zusatzaufgabe 7

In dieser Aufgabe rechnen wir in $\mathbb{Z}/11\mathbb{Z}$.

a) Stelle eine Tabelle auf, in der alle Potenzen $[2]^k$ mit $k = 1, 2, \ldots, 10$ aufgeführt sind. Ist $[2]$ eine Primitivwurzel?

b) Berechne den Bruch $\dfrac{[7]}{[8]}$, indem Du $[7]$ als Potenz $[2]^k$ (k aus der Tabelle ablesen) und entsprechend $[8]$ als Potenz von $[2]$ darstellst.

c) Bestimme für alle $[a] \in \mathbb{Z}/13\mathbb{Z}$ mit $[a] \neq 0$ das inverse Element $[a]^{-1}$.
Hinweis: Verfahre entsprechend zu Teil b) und verwende den kleinen Fermat.

17 Ausarbeitung Unterrichtsstunde 7: Asymmetrische Verschlüsselung

17.1 Stundenverlauf

Zeit	Unterrichtsschritte bzw. Unterrichtsarrangement	Sozialform L-S-Tätigkeit Methode	Was ich brauche
17:00	Wiederholung: Primitivwurzel, Kleiner Satz von Fermat, Brüche berechnen	L-S-Gespräch	Tafel
17:05	Übung Potenzen und kleiner Satz von Fermat	Einzel-/ Partnerarbeit	Arbeitsblatt 7.1
17:15	Besprechung	L-S-Gespräch	Visualizer
17:18	Elgamal-Verfahren, Begründung gemeinsam ergänzen	Lehrervortrag	Arbeitsblatt 7.2 Visualizer
17:25	Übung Elgamal-Verschlüsselung	Einzel-/ Partnerarbeit	Arbeitsblatt 7.3
17:40	Besprechung	L-S-Gespräch	Visualizer
17:43	Kongruenzgleichungen, Wiederholung verallgemeinerter euklidischer Algorithmus	L-S-Gespräch	Tafel
17:55	RSA-Verfahren	Lehrervortrag	Arbeitsblatt 7.4 Visualizer
18:00	Aufgabe 3 gemeinsam lösen	L-S-Gespräch	Arbeitsblatt 7.4 Visualizer
18:05	Übung RSA-Verfahren	Einzel-/ Partnerarbeit	Arbeitsblatt 7.4
18:18	Begründung RSA-Verfahren	Tafelvortrag	Tafel
18:30	Verabschiedung		

Anmerkungen: Aus Zeitgründen wurden die Prinzipien der Verschlüsselungsverfahren auf Arbeitsblättern dargestellt. Leider kommt dadurch nur die Begründung, warum das RSA-Verfahren funktioniert, in den Aufschrieb der Schüler:innen.

17.2 Tafelanschriebe

Potenztabelle für $\mathbb{Z}_7$:

$k=$	1	2	3	4	5	6
$[0]^k=$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]^k=$	$[1]$	$[1]$	$[1]$	$[1]$	$[1]$	$[1]$
$[2]^k=$	$[2]$	$[4]$	$[1]$	$[2]$	$[4]$	$[1]$
$[3]^k=$	$[3]$	$[2]$	$[6]$	$[4]$	$[5]$	$[1]$
$[4]^k=$	$[4]$	$[2]$	$[1]$	$[4]$	$[2]$	$[1]$
$[5]^k=$	$[5]$	$[4]$	$[6]$	$[2]$	$[3]$	$[1]$
$[6]^k=$	$[6]$	$[1]$	$[6]$	$[1]$	$[6]$	$[1]$

Primitivwurzel: Z.B. in $\mathbb{Z}_7$: $[3], [5]$.

Kleiner Satz von Fermat: Ist p Primzahl, $[a] \neq [0]$ in $\mathbb{Z}_p$, dann

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}_p.$$

Brüche berechnen: Sei p eine Primzahl und $[a] \neq [0]$ in $\mathbb{Z}_p$. Dann gilt

$$\frac{[1]}{[a]^k} = \frac{[a]^{p-1}}{[a]^k} = [a]^{p-1-k}.$$

Arbeitsblatt 7.1: Potenzen und kleiner Satz von Fermat (Besprechung an Tafel)

Arbeitsblatt 7.2: Prinzip der Elgamal-Verschlüsselung (Besprechung und Begründung am Visualizer)

Arbeitsblatt 7.3: Elgamal-Verschlüsselung (Besprechung an Tafel)

9. Kongruenzgleichungen

Beispiel: $x \cdot 9 \equiv 1 \mod 16 \qquad (*)$

Lösung: $(*) \Leftrightarrow 9x + 16y = 1$ für ein $y \in \mathbb{Z}$.

Verallgemeinerter euklidischer Algorithmus:

$$\begin{array}{rcl|rcl} 16 &=& 1\cdot 9 + 7 & 7 &=& 16 - 1\cdot 9 \\ 9 &=& 1\cdot 7 + 2 & 2 &=& 9 - 1\cdot 7 \\ 7 &=& 3\cdot 2 + 1 & 1 &=& 7 - 3\cdot 2 = 7 - 3(9 - 1\cdot 7) \\ & & & & = & 4\cdot 7 - 3\cdot 9 = 4(16 - 1\cdot 9) - 3\cdot 9 \\ & & & & = & 4\cdot 16 - 7\cdot 9 \end{array}$$

$\Rightarrow$ $(x, y) = (-7 \mid 4)$ ist eine Lösung.

Alle Lösungen: $(x, y) = (-7 + 16k \mid 4 - 9k)$ mit $k \in \mathbb{Z}$.

$\Rightarrow$ Alle Lösungen von $(*)$: $x = -7 + 16k$ mit $k \in \mathbb{Z}$.

Arbeitsblatt 7.4: Das RSA-Verfahren (Besprechung und erste Aufgabe am Visualizer)

Arbeitsblatt 7.5: RSA-Verschlüsselung knacken (Besprechung an Tafel)

10. RSA-Verschlüsselung

Seien $p, q, m, \widetilde{m}, e, v, n, N$ gemäß dem RSA-Algorithmus gewählt bzw. berechnet.

Wir beweisen, dass $\boxed{N^e \equiv n \mod m}$ gilt.

Kleiner Fermat: Ist p Primzahl und $a \in \mathbb{N}$ kein Vielfaches von p, so gilt $a^{p-1} \equiv 1 \mod p$.

Vorbemerkung 1: $\underbrace{a \equiv n \mod p}_{a-n \text{ durch } p \text{ teilbar}}$ und $\underbrace{a \equiv n \mod q}_{a-n \text{ durch } q \text{ teilbar}} \overset{p,q \text{ Primzahlen}}{\Leftrightarrow} a \equiv n \mod \underbrace{pq}_{=m}$.

Vorbemerkung 2: $e \cdot v \equiv 1 \mod \widetilde{m}$
$\Leftrightarrow\ e \cdot v = 1 + k\widetilde{m} = 1 + k(p-1)(q-1)$ mit einem $k \in \mathbb{Z}$.

Wir rechnen zunächst nur modulo p.
Vorbemerkung 1 $\Rightarrow\ N^e \equiv (n^v)^e = n^{e \cdot v} \mod p$

Fall $\mathrm{ggT}(n, p) = 1$:

$$n^{e \cdot v} \overset{\text{Vorbemerkung 2}}{=} n^{1+k(p-1)(q-1)} = n \cdot \left(n^{p-1}\right)^{k(q-1)} \overset{\substack{\text{kleiner} \\ \text{Fermat}}}{\equiv} n \cdot 1^{k(q-1)} = n \mod p$$

Fall $\mathrm{ggT}(n, p) = p$: Dann ist $n = l \cdot p$ und somit $n \equiv 0 \mod p$.
$\Rightarrow\ n^{e \cdot v} \equiv 0^{e \cdot v} = 0 \equiv n \mod p$.

In beiden Fällen gilt also

$$N^e \equiv n^{e \cdot v} \equiv n \mod p. \tag{1}$$

Nun rechnen wir nur modulo q. Indem man p und q vertauscht, folgt genauso, dass

$$N^e \equiv n^{e \cdot v} \equiv n \mod q \tag{2}$$

gilt.

(1) und (2) $\overset{\substack{\text{Vorbemerkung 1} \\ \Rightarrow \\ pq=m}}{}$ $\boxed{N^e \equiv n \mod m}$. $\square$

17.3 Arbeitsblätter

Siehe folgende Seiten

Potenzen und kleiner Satz von Fermat

Aufgabe 1

Berechne die folgenden Potenzen möglichst geschickt ohne Taschenrechner:

a) $[4]^{-11}$ in $\mathbb{Z}_{13}$:

b) $[6]^{31}$ in $\mathbb{Z}_{29}$:

c) $[6]^{32}$ in $\mathbb{Z}_{29}$:

Zusatzaufgabe 1

Für diese Aufgabe benützen wir eine Potenztabelle für $\mathbb{Z}_{11}$.

$k=$	1	2	3	4	5	6	7	8	9	10
$[2]^k=$	$[2]$	$[4]$	$[8]$	$[5]$	$[10]$	$[9]$	$[7]$	$[3]$	$[6]$	$[1]$
$[4]^k=$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

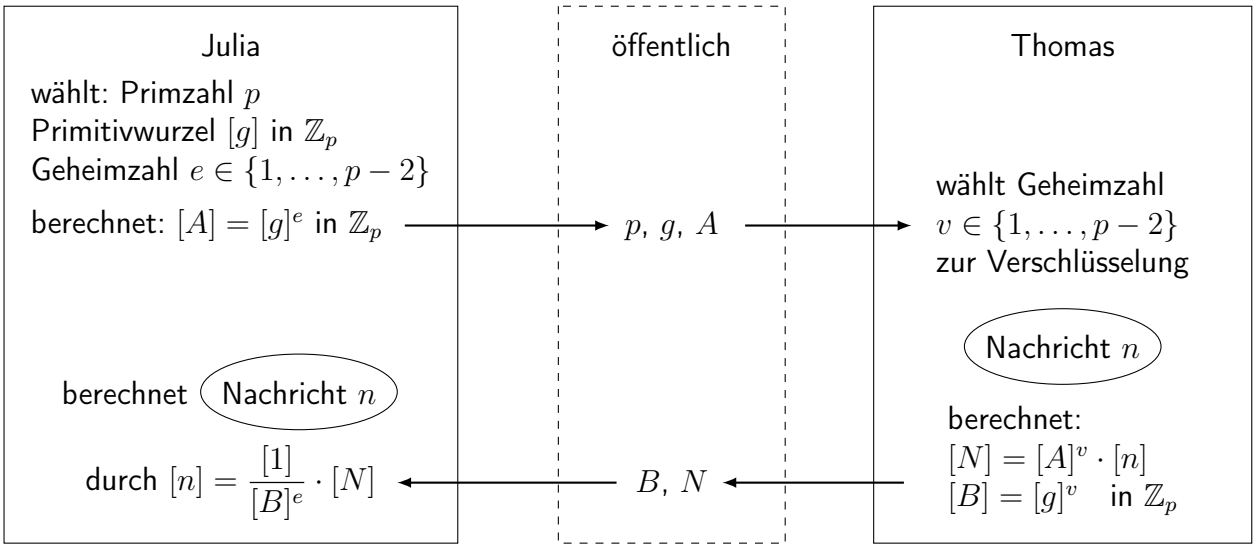
a) Trage in die Tabelle die Potenzen von $[4]$ in $\mathbb{Z}_{11}$ ein. Wie viele verschiedene Elemente von $\mathbb{Z}_{11}$ können durch $[4]^k$ dargestellt werden? Warum ist $[4]$ keine Primitivwurzel?

b) Wie hängen die Zeile für $[4]^k$ und die Zeile für $[2]^k$ zusammen?

c) Sei p eine Primzahl mit $p \geq 3$ und $[n^2]$ eine Quadratzahl in $\mathbb{Z}_p$ mit $[n] \neq 0$. Folgere aus dem kleinen Satz von Fermat dass $[n^2]^{(p-1)/2} = [1]$ gilt.

d) Sei p eine Primzahl mit $p \geq 3$. Wie viele verschiedene Elemente von $\mathbb{Z}_p$ können höchstens durch $[n^2]^k$ mit $k \in \mathbb{N}$ dargestellt werden? Warum ist $[n^2]$ keine Primitivwurzel?

Prinzip der Elgamal-Verschlüsselung



Begründung:

Elgamal-Verschlüsselung

Aufgabe 2

Julia wählt $p = 23$ und die Primitivwurzel $[5]$ in $\mathbb{Z}_{23}$. Weiter wählt sie den Entschlüsselungsexponent $e = 14$ und berechnet

$$[A] = [5]^{14} = [25]^7 = [25 - 23]^7 = [2]^7 = [128] = [128 - 115] = [13] \text{ in } \mathbb{Z}_{23}.$$

Julia veröffentlicht auf ihrer Homepage $(p, g, A) = (23, 5, 13)$.

a) Thomas möchte die Nachricht $n = 11$ an Julia senden. Dazu wählt er den Verschlüsselungsexponent $v = 3$ und berechnet in $\mathbb{Z}_{23}$

$[B] = [g]^v = [5]^3 =$ in $\mathbb{Z}_{23}$,

$[A]^v = [13]^3 =$ in $\mathbb{Z}_{23}$,

$[N] = [A]^v \cdot [n] = [12] \cdot [11] =$ in $\mathbb{Z}_{23}$.

Thomas schickt also $(B = \quad , N = \quad)$ an Julia.
Julia berechnet als erstes $[B]^{-14} = [B]^{22-14} = [B]^8 = [B^2]^4 = [B^2 - 92]^4 =$

in $\mathbb{Z}_{23}$.

Hinweis: $[18] = [-5]$ kann hilfreich sein.
Dann erhält sie die Nachricht n durch Multiplikation:

$[n] = [B]^{-14} \cdot [N] =$ in $\mathbb{Z}_{23}$.

b) Marc schickt an Julia $(B, N) = (3, 21)$. Welche Nachricht n hat er an Julia geschickt?

$[B]^{-14} =$ in $\mathbb{Z}_{23}$,

$[n] =$ in $\mathbb{Z}_{23}$.

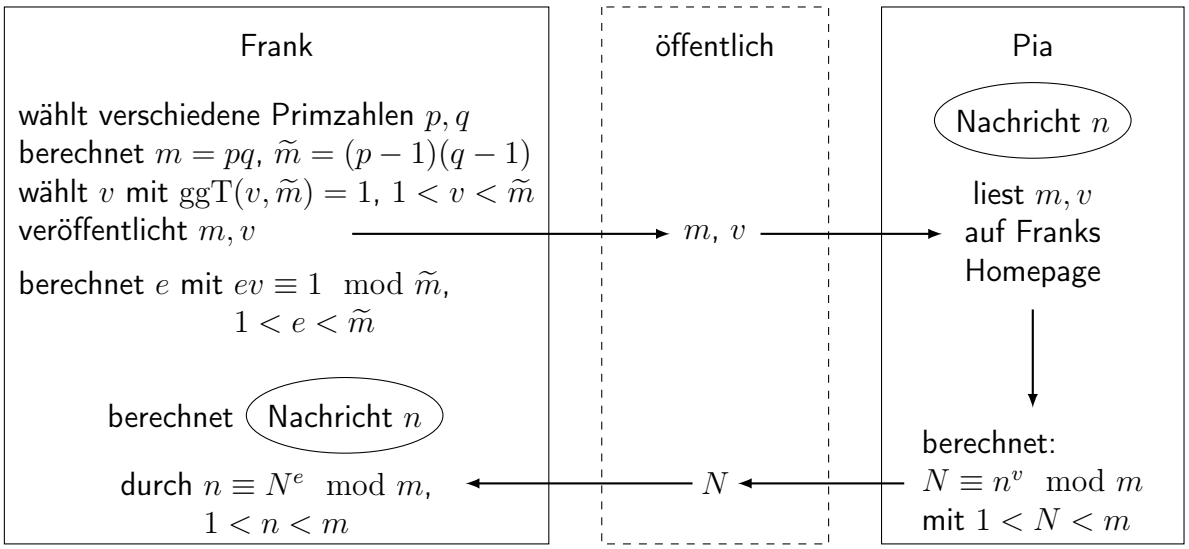
c) Zusatzaufgabe: Erstelle die Potenztabelle für $[5]^k$ um herauszufinden, welchen Verschlüsselungsexponent Marc gewählt hat.
Kennzeichne Marcs Verschlüsselungsexponent durch Umkringeln.

$k =$	1	2	3	4	5	6	7	8	9	10	11
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

$k =$	12	13	14	15	16	17	18	19	20	21	22
$[5]^k =$	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Das RSA-Verfahren

(von Rivest, Shamir, Adleman)



Aufgabe 3

Frank wählt: $p = 3$, $q = 11$,

berechnet: $m =$, $\widetilde{m} =$

wählt: Verschlüsselungsexponent $v = 7$ (erfüllt $1 < v < \widetilde{m}$ und $\mathrm{ggT}(v, \widetilde{m}) = 1$)

veröffentlicht: $m =$ und $v = 7$

berechnet: e:

Pia liest die Homepage von Frank und will ihm die Nachricht $\boxed{n = 6}$ übermitteln. Sie berechnet Modulo 33: $n^v = 6^7 =$

und schickt Frank $\boxed{N =}$. Frank liest in Pias Mail $\boxed{N =}$ und berechnet Modulo 33: $N^e =$

erhält also $\boxed{n =}$ zurück.

RSA-Verschlüsselung knacken

Aufgabe 4

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 55$ und $v = 7$. Er erhält von Peter die Zahl $N = 25$.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Zusatzaufgabe 2

Frank veröffentlicht auf seiner Homepage die Zahlen $m = 51$ und $v = 3$. Er erhält von Jane die Zahl $N = 8$ als verschlüsselte Botschaft.

Bestimme $p, q, \widetilde{m}, e$ und die entschlüsselte Botschaft n.

Schriftliche Aufgaben

Name:

Aufgabe 5

Gegeben ist die Kongruenzgleichung

$$21x \equiv a \mod 51, \tag{1}$$

wobei $a \in \mathbb{N}$ später gewählt wird.

a) Gib eine zu (1) äquivalente diophantische Gleichung an.

$\square$ mit $y \in \mathbb{Z}$. (2)

b) Welche Bedingung müssen a und $\mathrm{ggT}(21, 51)$ erfüllen, damit die diophantische Gleichung (2) Lösungen besitzt?

Bedingung: $\square$.

c) Kreuze in der Tabelle an, für welche der gegebenen Zahlen a die Kongruenzgleichung (1) jeweils Lösungen besitzt.

$a =$	1	3	7	17	21	51
(1) besitzt Lösungen						

Weiter auf Seite 2

Aufgabe 6

Gegeben ist die Kongruenzgleichung

$$e \cdot 7 \equiv 1 \mod 60. \tag{3}$$

a) Gib eine zu (3) äquivalente diophantische Gleichung an.

$\square$ mit $y \in \mathbb{Z}$. (4)

b) Berechne mit Hilfe des erweiterten euklidischen Algorithmus eine Lösung von (4).

Erweiterter euklidischer Algorithmus:

Eine Lösung von (4): $(e \mid y) =$ $\square$.

c) Gib alle ganzzahligen Lösungen von (4) an.

$(e \mid y) =$ $\square$ mit $k \in \mathbb{Z}$.

d) Gib alle Lösungen von (3) an. $e =$ $\square$.

e) Gib die einzige Lösung x von (3) an, für die $1 < x < 60$ gilt.

$e =$ $\square$.

f) Mache die Probe. $e \cdot 7 =$ $\square$ $=$ $\square$ $\cdot 60 + 1$.

Weiter auf Seite 3

Aufgabe 7

Noah möchte sich Nachrichten schicken lassen, die mit dem Elgamal-Verfahren verschlüsselt sind. Er wählt $p = 31$, $g = 11$, $e = 24$ und berechnet

$$\begin{aligned} [11]^2 &= [121 - 124] = [-3], \\ [11]^6 &= [-3]^3 = [-27] = [4], \\ [A] &= [11]^{24} = [4]^4 = [64] \cdot [4] = [2] \cdot [4] = [8] \text{ in } \mathbb{Z}_{31}. \end{aligned}$$

Er veröffentlich also auf seiner Homepage $p = 31$, $g = 11$ und $A = 8$.

a) Anna möchte die Nachricht $n = 10$ für Noah verschlüsseln. Sie wählt den Verschlüsselungsexponent $v = 4$ und berechnet in $\mathbb{Z}_{31}$

$[B] =$ ☐, $[A]^4 =$ ☐, $[N] =$ ☐.

b) Emilia schickt an Noah $B = 4$ und $N = 3$. Berechne

$[B]^{-e} =$ ☐, $[n] =$ ☐ in $\mathbb{Z}_{31}$.

Aufgabe 8

Frank veröffentlicht auf seiner Homepage $m = 77$ und $v = 43$, damit Personen ihre Nachrichten an ihn mit RSA verschlüsseln können..

a) Gib die Werte an, die er gewählt bzw. berechnet hat.

$p =$ ☐, $q =$ ☐, $\widetilde{m} =$ ☐, $e =$ ☐ (beachte die vorigen Aufgaben).

b) Andrew schickt Frank die Zahl $N = 2$. Entschlüssle die Nachricht.

$n =$ ☐.